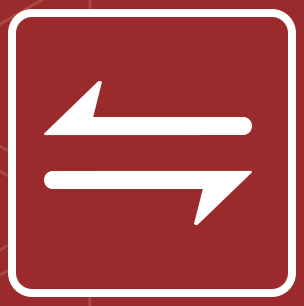


FORTINET
High Performance Network Security

FortiSwitch Devices Managed by FortiOS 5.6

FORTIOS
5.6
VERSION

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FORTINET PRIVACY POLICY

https://www.fortinet.com/corporate/about-us/privacy.html

FEEDBACK

Email: techdocs@fortinet.com

Thursday, January 18, 2018

FortiSwitch Devices Managed by FortiOS 5.6

TABLE OF CONTENTS

Change log

Date	Change Description
December 6, 2017	Initial document release for FortiOS 5.6.3
December 14, 2017	Added the following note in the “Network topologies for managed FortiSwitches” chapter: “Using the hardware or software switch interface in FortiLink mode is not recommended in most cases. It can be used when the traffic on the ports is very light because all traffic across the switches moves through FortiGate.”
December 21, 2017	Updates made to the following sections: • “Supported models” • “What’s new for managed FortiSwitches in FortiOS 5.6.3 with FortiSwitch 3.6.3 (and later releases)” • “Miscellaneous configuration option changes” • “Transitioning from a FortiLink split interface to a FortiLink MCLAG”
January 18, 2018	Made the switches-per-FortiGate tables consistent in “Introduction.”

Introduction

NOTE: FortiLink is not supported in Transparent mode.

The maximum number of supported FortiSwitches depends on the FortiGate model:

FortiGate Model Range	Number of FortiSwitches Supported
Up to FortiGate-98 and FortiGate-VM01	8
FortiGate-100 to 280 and FortiGate-VM02	24
FortiGate-300 to 5*xx*	48
FortiGate-600 to 900 and FortiGate-VM04	64
FortiGate-1000 and up	128
FortiGate-3*xxx* and up, and FortiGate-VM08 and up	256

Supported models

The following table shows the FortiSwitch models that support FortiLink mode when paired with the corresponding FortiGate models and the listed minimum software releases.

FortiGate and FortiWiFi Models	Earliest FortiOS	FortiSwitch Models
FGT-90D	5.2.2	FS-224D-POE
FGT-60D FGT-100D, 140D, 140D-POE, 140D-T1 FGT-200D, 240D, 280D, 280D-POE FGT-600C FGT-800C FGT-1000C, 1200D, 1500D FGT-3700D, FGT-3700DX	5.2.3	FSR-112D-POE FS-108D-POE FS-124D (POE) FS-224D-POE and FPOE
	5.4.0	All FortiSwitch D-series models. FortiSwitchOS 3.3.x or 3.4.0 is recommended.

FortiGate and FortiWiFi Models	Earliest FortiOS	FortiSwitch Models
FGT and FWF-30D, 30D-POE, 30E FGT and FWF-50E, 51E FGR-60D FGT-70D, 70D-POE FGT-80D FGR-90D FGT and FWF-92D FGT-94D-POE, 98D-POE FGT-300D FGT-400D FGT-500D FGT-600D FGT-900D FGT-1000D FGT-3000D, 3100D, 3200D, 3240C, 3600C, 3810D, 3815D FGT_VM, VM64, VM64-AWS, VM64-AWSONDEMAND, VM64-HV, VM64-KVM, VM-VMX, VM64-XEN	5.4.1	All FortiSwitch D-series models. FortiSwitchOS 3.4.2 or later is required for all managed switches.
FGT and FWF- 60E, 61E FGT-100E, 101E	5.4.2	All FortiSwitch D-series models. FortiSwitch 3.4.2 or later is required for all managed switches.
FGT-80E, 80E-POE, 81E, 81E-POE FGT-100EF	5.4.3	All FortiSwitch D-series models. FortiSwitch 3.4.2 or later is required for all managed switches.
FGT-90E, 91E FGT-200E, 201E FGT-2000E, 2500E	5.6.0	All FortiSwitch D-series models. FortiSwitch 3.5.4 or later is required for all managed switches.
FGT-500E	5.6.3	All FortiSwitch D-series and E-series models. FortiSwitch 3.6.0 or later is required for all managed switches.

Refer to Introduction on page 8 for details about the features supported on each FortiSwitch model.

Before you begin

Before you start administrating your FortiSwitch unit, it is assumed that you have completed the initial configuration of the FortiSwitch unit, as outlined in the QuickStart Guide for your FortiSwitch model and have administrative access to the FortiSwitch unit's Web-based manager and CLI.

What's new for managed FortiSwitches in FortiOS 5.6.3 with FortiSwitch 3.6.3 (and later releases)

This section describes new managed FortiSwitch features in FortiOS 5.6.3 with FortiSwitch 3.6.3.

Firewall policy now required for RADIUS traffic (434470)

In FortiLink mode, you must manually create a firewall policy to allow RADIUS traffic for 802.1x authentication from the FortiSwitch (for example, from the FortiLink interface) to the RADIUS server through the FortiGate.

STP root guard (376015)

Enable root guard on all ports that should not be root bridges. Do not enable root guard on the root port. You must have STP enabled to be able to use root guard.

Using the FortiGate GUI

1. Go to **WiFi & Switch Controller > Managed FortiSwitch**.
2. Right-click on a port.
3. Select **Enable** or **Disable**.

Using the FortiGate CLI

```
config switch-controller managed-switch
   edit <switch-id>
      config ports
         edit <port name>
            set stp-root-guard {enabled | disabled}
         end
      end
```

STP BPDU guard (406182)

When BPDU guard is enabled on STP edge ports, any BPDUs received cause the ports to go down for a specified number of minutes. The BPDUs are not forwarded, and the network edge is enforced.

There are two prerequisites for using BPDU guard:

- You must define the port as an edge port with the `set edge-port enable` command.
- You must enable STP on the switch interface with the `set stp-state enabled` command.

Using the FortiGate GUI

1. Go to **WiFi & Switch Controller > Managed FortiSwitch**.
2. Right-click on a port.
3. Select **Enable** or **Disable**.

Using the FortiGate CLI

```
config switch-controller managed-switch
   edit <switch-id>
      config ports
         edit <port name>
            set stp-bpdu-guard {enabled | disabled}
            set stp-bpdu-guard-time <0-120>
         end
      end
```

FortiSwitch log message changes (438738)

More details are now provided in exported FortiSwitch logs, for example:

- New Switch-Controller user field and daemon-name ui fields.
- Removed Switch-Controller keyword from the msg field
- Changed UpdSwConf keyword in msg field to FortiSwitch in flcfgd logs
- Removed the VDOM keyword from the msg field in flcfgd logs
- Removed the Fortiswitch keyword before SN in the msg field
- Changed syslog to have switch SN first followed by a space and then the first word following with a capital (in the msg field)

Use the following CLI commands to enable the export of FortiSwitch logs and to set the level of logging included. The system logs all messages at and above the logging severity level you select. For example, if you select `error`, the system logs error, critical, alert, and emergency level messages.

```
config switch-controller switch-log
   set status (*enable | disable)
   set severity [emergency | alert | critical | error | warning | notification |
       *information | debug]
end
```

Support FSW BPDU Guard (442921) (442922)

With standard STP, a device that sends BPDU(s) to any switch port becomes a member of that switch's STP network topology. In order to enforce a network edge, the access ports on the switch can be configured with BPDU guard. With BPDU guard enabled, the port does not forward BPDUs upstream (toward its root bridge). Instead, when a BPDU guard enabled port receives any BPDU, it immediately puts the port into a blocking state and alerts the user.

This prevents the access port from accepting the downstream device, removing it from the receiving switch's STP calculations. In order to unblock the port after bpdu guard has triggered, the user must execute a reset command. After the port is reset, it will resume normal operation and return to a blocking state only if another BPDU is received.

BPDU guard is typically used in conjunction with Root Guard to enforce a specific network topology.

Syntax

```
config switch-controller managed-switch
   edit <switch SN>
      config ports
         edit <port>
            set stp-bpdu-guard <enable | *disable>
            set stp-bpdu-guard-timeout <time> (0-120 in minutes)
         next
      end
   next
end

config switch-controller managed-switch
   edit <switch SN>
      config ports
         edit <port>
            set stp-root-guard <enable | *disable>
         next
      end
   next
end

diagnose switch-controller dump stp <switch SN> <instance>
diagnose switch-controller bpdu-guard-status <switch SN>
```

Managed switch CLI features added to GUI (448722)

Added new optional columns "Edge Port", "LLDP Profile", "QoS Policy", "STP BPDU Guard", "STP Root Guard" in **WiFi & Switch Controller > FortiSwitch Ports**.

This would allow administrators to make changes to the features above to multiple switch ports at the same time.

Added unit in help-text when setting max-rate/min-rate under switch-controller qos queue-policy (449487) (449869)

Modified the CLI help-text on the FortiGate to show priority under strict schedule when setting max-rate/min-rate under switch-controller qos queue-policy.

Syntax

```
set priority-0
   queue-0 COS queue 0. (lowest priority)
   queue-1 COS queue 1.
   queue-2 COS queue 2.
   queue-3 COS queue 3.
   queue-4 COS queue 4.
   queue-5 COS queue 5.
   queue-6 COS queue 6.
   queue-7 COS queue 7. (highest priority)
```

Added FortiSwitch factory-reset functionality to the FortiOS GUI (393205)

Added a **Factory Reset** button to the **WiFi & Switch Controller > Managed FortiSwitch** page when a FortiSwitch document is selected.

Syntax

```
execute switch-controller factory-rest <switch sn>
```

What's new for managed FortiSwitches in FortiOS 5.6.1 with FortiSwitch 3.6.0 (and later releases)

This section describes new managed FortiSwitch features in FortiOS 5.6.1 with FortiSwitch 3.6.0.

Simplified method to convert a FortiSwitch to standalone mode (393205)

There is an easier way to convert a FortiSwitch from FortiLink mode to standalone mode so that it will no longer be managed by a FortiGate:

- `execute switch-controller factory-reset <switch-id>`
  This command returns the FortiSwitch to the factory defaults and then reboots the FortiSwitch. If the FortiSwitch is configured for FortiLink auto-discovery, FortiGate can detect and automatically authorize the FortiSwitch.
- `execute switch-controller set-standalone <switch-id>`
  This command returns the FortiSwitch to the factory defaults, reboots the FortiSwitch, and prevents the FortiGate from automatically detecting and authorizing the FortiSwitch.

You can disable FortiLink auto-discovery on multiple FortiSwitches using the following commands:

```
config switch-controller global
   set disable-discovery <switch-id>
end
```

You can also add or remove entries from the list of FortiSwitches that have FortiLink auto-discovery disabled using the following commands:

```
config switch-controller global
   append disable-discovery <switch-id>
   unselect disable-discovery <switch-id>
end
```

Quarantines (410828)

Quarantined MAC addresses are blocked on the connected FortiSwitches from the network and the LAN.

NOTE: You must enable the quarantine feature in the FortiGate CLI using the `set quarantine enable` command. You can add MAC addresses to the quarantine list before enabling the quarantine feature, but the quarantine does not go into effect until enabled.

Quarantining a MAC address

Using the FortiGate GUI

1. Select the host to quarantine.
   - Go to **Security Fabric > Physical Topology**, right-click on a host, and select **Quarantine Host on FortiSwitch**.
   - Go to **Security Fabric > Logical Topology**, right-click on a host, and select **Quarantine Host on FortiSwitch**.
   - Go to **FortiView > Sources**, right-click on an entry in the Source column, and select **Quarantine Host on FortiSwitch**.
2. Click **OK** to confirm that you want to quarantine the host.

Using the FortiGate CLI

```
config switch-controller quarantine
   set quarantine enable
      edit <MAC_address>
         set description <string>
         set tags <tag1 tag2 tag3 ...>
      next
   next
end
```

Option	Description
MAC_address	A layer-2 MAC address in the following format: `12:34:56:aa:bb:cc`
string	Optional. A description of the MAC address being quarantined.
tag1 tag2 tag3 …	Optional. A list of arbitrary strings.

Viewing quarantine entries

Quarantine entries are created on the FortiGate that is managing the FortiSwitch.

Using the FortiGate GUI

1. Go to **Monitor > Quarantine Monitor**.
2. Click **Quarantined on FortiSwitch**.

Using the FortiGate CLI

Use the following command to view the quarantine list of MAC addresses:

```
show switch-controller quarantine
```

When the quarantine feature is enabled on the FortiGate, it creates a quarantine VLAN (qtn.<FortiLink_port_name>) on the virtual domain. The quarantine VLAN is applied to the allowed and untagged VLANs on all connected FortiSwitch ports.

Use the following command to view the quarantine VLAN:

```
show system interface qtn.<FortiLink_port_name>
```

Use the following command to view how the quarantine VLAN is applied to the allowed and untagged VLANs on all connected FortiSwitch ports:

```
show switch-controller managed-switch
```

Releasing MAC addresses from quarantine

Using the FortiGate GUI

1. Go to **Monitor > Quarantine Monitor**.
2. Click **Quarantined on FortiSwitch**.
3. Right-click on one of the entries and select **Delete** or **Remove All**.
4. Click **OK** to confirm your choice.

Using the FortiGate CLI

Use the following commands to delete a quarantined MAC address:

```
config switch-controller quarantine
config targets
   delete <MAC_address>
end
```

When the quarantine feature is disabled, all quarantined MAC addresses are released from quarantine. Use the following commands to disable the quarantine feature:

```
config switch-controller quarantine
   set quarantine disable
end
```

Assign untagged VLANs to a managed FortiSwitch port (410828)

Use the following commands to assign untagged VLANs to a managed FortiSwitch port:

```
config switch-controller managed-switch
   edit <managed-switch>
      config ports
         edit <port>
            set untagged-vlans <VLAN-name>
         next
      end
   next
end
```

View, create, and assign multiple 802.1X policy definitions (408389 and 403901)

Previously, you could create one 802.1X policy for all managed FortiSwitches in a virtual domain. Now, you can create multiple 802.1X policies and assign a different 802.1X policy to each managed FortiSwitch port.

View security policies for managed FortiSwitches

You can view security policies for managed FortiSwitches in two places:

- Go to **WiFi & Switch Controller > FortiSwitch Security Policies**.
- Go to **WiFi & Switch Controller > FortiSwitch Ports** and click the **+** next to a FortiSwitch. The security policy for each port is listed in the Security Policy column.

Create and assign multiple 802.1X policy definitions for managed FortiSwitches

Previously, you could create one 802.1X policy for all managed FortiSwitches in a virtual domain. Now, you can create multiple 802.1X policies and assign a different 802.1X policy to each managed FortiSwitch port.

To create an 802.1X security policy:

1. Go to **WiFi & Switch Controller > FortiSwitch Security Policies**.
2. Click **Create New**.
3. Enter a name for the new FortiSwitch security policy.
4. For the security mode, select **Port-based** or **MAC-based**.
5. Click **+** to select which user groups will have access.
6. Enable or disable guest VLANs on this interface to allow restricted access for some users.
7. Enter the number of seconds for authentication delay for guest VLANs. The range is 60-900 seconds.
8. Enable or disable authentication fail VLAN on this interface to allow restricted access for users who fail to access the guest VLAN.
9. Enable or disable MAC authentication bypass (MAB) on this interface.
10. Enable or disable EAP pass-through mode on this interface.
11. Enable or disable whether the session timeout for the RADIUS server will overwrite the local timeout.
12. Click **OK**.

To apply an 802.1X security policy to a managed FortiSwitch port:

1. Go to **WiFi & Switch Controller > FortiSwitch Ports**.
2. Click the **+** next to a FortiSwitch.
3. In the Security Policy column for a port, click + to select a security policy.
4. Click **OK** to apply the security policy to that port.

Override 802.1X settings

To override the 802.1X settings for a virtual domain:

1. Go to **WiFi & Switch Controller > Managed FortiSwitch**.
2. Click on a FortiSwitch faceplate and click **Edit**.
3. In the Edit Managed FortiSwitch page, move the **Override 802-1X settings** slider to the right.
4. In the Reauthentication Interval field, enter the number of minutes before reauthentication is required. The maximum interval is 1,440 minutes. Setting the value to 0 minutes disables reauthentication.
5. In the Max Reauthentication Attempts field, enter the maximum times that reauthentication is attempted. The maximum number of attempts is 15. Setting the value to 0 disables reauthentication.
6. Select **Deauthenticate** or **None** for the link down action. Selecting **Deauthenticate** sets the interface to unauthenticated when a link is down, and reauthentication is needed. Selecting **None** means that the interface does not need to be reauthenticated when a link is down.
7. Click **OK**.

Enable and disable switch-controller access VLANs through FortiGate (406718)

Access VLANs are VLANs that aggregate client traffic solely to the FortiGate. This prevents direct client-to-client traffic visibility at the layer-2 VLAN layer. Clients can only communicate with the FortiGate. After the client traffic reaches the FortiGate, the FortiGate can then determine whether to allow various levels of access to the client by shifting the client's network VLAN as appropriate.

Use `enable` to allow traffic only to and from the FortiGate and to block FortiSwitch port-to-port traffic on the specified VLAN. Use `disable` to allow normal traffic on the specified VLAN.

```
config system interface
   edit <VLAN name>
      set switch-controller-access-vlan {enable | disable}
   next
end
```

Override the admin password for all managed FortiSwitches (416261)

By default, each FortiSwitch has an admin account without a password. To replace the admin passwords for all FortiSwitches managed by a FortiGate, use the following commands:

```
config switch-controller switch-profile
   edit default
      set login-passwd-override {enable | disable}
      set login-passwd <password>
   next
end
```

If you had already applied a profile with the override enabled and the password set and then decide to remove the admin password, you need to apply a profile with the override enabled and use the `unset login-passwd` command; otherwise, your previously set password will remain in the FortiSwitch.

Configure an MCLAG with managed FortiSwitches (366617)

To configure a multichassis LAG (MCLAG) with managed FortiSwitches:

1. For each MCLAG peer switch, log into the FortiSwitch to create a LAG:

```
config switch trunk
   edit "LAG-member"
      set mode lacp-active
      set mclag-icl enable
      set members "<port>" "<port>"
   next
```

2. Enable the MCLAG on each managed FortiSwitch:

```
config switch-controller managed-switch
   edit "<switch-id>"
      config ports
         edit "<trunk name>"
            set type trunk
            set mode {static | lacp-passive | lacp-active}
            set bundle {enable | disable}
```

```
            set members "<port>,<port>"
            set mclag {enable | disable}
         next
      end
   next
```

3. Log into each managed FortiSwitch to check the MCLAG configuration:

```
diagnose switch mclag
```

After the FortiSwitches are configured as MCLAG peer switches, any port that supports advanced features on the FortiSwitch can become a LAG port. When `mclag` is enabled and the LAG port names match, an MCLAG peer set is automatically formed. The member ports for each FortiSwitch in the MCLAG do not need to be identical to the member ports on the peer FortiSwitch.

Configure QoS with managed FortiSwitches (373581)

Quality of Service (QoS) provides the ability to set particular priorities for different applications, users, or data flows. **NOTE:** FortiGate does not support QoS for hard or soft switch ports.

To configure the QoS for managed FortiSwitches:

1. Configure a Dot1p map.

```
config switch-controller qos dot1p-map
   edit <Dot1p map name>
      set description <text>
      set priority-0 <queue number>
      set priority-1 <queue number>
      set priority-2 <queue number>
      set priority-3 <queue number>
      set priority-4 <queue number>
      set priority-5 <queue number>
      set priority-6 <queue number>
      set priority-7 <queue number>
   next
end
```

2. Configure a DSCP map.

```
config switch-controller qos ip-dscp-map
   edit <DSCP map name>
      set description <text>
      configure map <map_name>
         edit <entry name>
            set cos-queue <COS queue number>
            set diffserv {CS0 | CS1 | AF11 | AF12 | AF13 | CS2 | AF21 | AF22 | AF23
                | CS3 | AF31 | AF32 | AF33 | CS4 | AF41 | AF42 | AF43 | CS5 | EF |
                CS6 | CS7}
            set ip-precedence {network-control | internetwork-control | critic-ecp
                | flashoverride | flash | immediate | priority | routine}
            set value <DSCP raw value>
         next
      end
   end
```

3. Configure the egress QoS policy.

```
config switch-controller qos queue-policy
   edit <QoS egress policy name>
      set schedule {strict | round-robin | weighted}
      config cos-queue
      edit [queue-<number>]
         set description <text>
         set min-rate <rate in kbps>
         set max-rate <rate in kbps>
         set drop-policy {taildrop | random-early-detection}
         set weight <weight value>
         next
      end
   next
end
```

4. Configure the overall policy that will be applied to the switch ports.

```
config switch-controller qos qos-policy
   edit <QoS egress policy name>
      set default-cos <default CoS value 0-7>
      set trust-dot1p-map <Dot1p map name>
      set trust-ip-dscp-map <DSCP map name>
      set queue-policy <queue policy name>
   next
end
```

5. Configure each switch port.

```
config switch-controller managed-switch
   edit <switch-id>
      config ports
         edit <port>
            set qos-policy <CoS policy>
         next
      end
   next
end
```

Reset PoE-enabled ports from the GUI (387417)

If you need to reset PoE-enabled ports, go to **WiFi & Switch Control > FortiSwitch Ports**, right-click on one or more PoE-enabled ports and select **Reset PoE** from the context menu.

You can also go to **WiFi & Switch Control > Managed FortiSwitch** and click on a port icon for the FortiSwitch of interest. In the FortiSwitch Ports page, right-click on one or more PoE-enabled ports and select **Reset PoE** from the context menu.

Adding preauthorized FortiSwitches (382774)

After you preauthorize a FortiSwitch, you can assign the FortiSwitch ports to a VLAN.

To preauthorize a FortiSwitch:

1. Go to **WiFi & Switch Controller** > **Managed FortiSwitch**.
2. Click **Create New**.
3. In the New Managed FortiSwitch page, enter the serial number, model name, and description of the FortiSwitch.
4. Move the **Authorized** slider to the right.
5. Click **OK**.
   The Managed FortiSwitch page shows a FortiSwitch faceplate for the preauthorized switch.

What's new for managed FortiSwitches in FortiOS 5.6 with FortiSwitch 3.6.0 (and later releases)

IGMP snooping (387515)

The GUI and CLI support the ability to configure IGMP snooping for managed switch ports.

To enable IGMP snooping from the GUI, go to **WiFi & Switch Controller > FortiSwitch VLANs**, edit a VLAN and turn on **IGMP Snooping** under **Networked Devices**.

From the CLI, start by enabling IGMP snooping on the FortiGate:

```
config switch-controller igmp-snooping
   set aging-time <int>
   set flood-unknown-multicast (enable | disable)
end
```

Then enable IGMP snooping on a VLAN:

```
config system interface
   edit <vlan>
      set switch-controller-igmp-snooping (enable | disable)
end
```

Use the following command to enable IGMP snooping on switch ports, and to override the global parameters for a specific switch.

```
config switch-controller managed-switch
   edit <switch>
      config ports
         edit port <number>
            set igmp-snooping (enable | disable)
            set igmps-flood-reports (enable | disable)
         next
      config igmp-snooping globals
         set aging-time <int>
         set flood-unknown-multicast (enable | disable)
      end
   next
end
```

User-port link aggregation groups (378470)

The GUI now supports the ability to configure user port LAGs on managed FortiSwitches.

To create a link aggregation group for FortiSwitch user ports:

1. Go to **WiFi & Switch Controller** > **FortiSwitch Ports**
2. Click **Create New > Trunk**.
3. In the New Trunk Group page:
   a. Enter a name for the trunk group
   b. Select two or more physical ports to add to the trunk group
   c. Select the mode: Static, Passive LACP, or Active LACP
4. Click **OK**.

DHCP blocking, STP, and loop guard on managed FortiSwitch ports (375860)

The managed FortiSwitch GUI now supports the ability to enable/disable DHCP blocking, STP and loop guard for FortiSwitch user ports.

Go to to **WiFi & Switch Controller** > **FortiSwitch Ports.** For any port you can select DHCP Blocking, STP, or Loop Guard. STP is enabled on all ports by default. Loop guard is disabled by default on all ports.

Switch profile enhancements (387398)

Defaults switch profiles are bound to every switch discovered by the FortiGate. This means that an administrator can establish a password for this profile or create a new profile and bind that profile to any switch. Consquently, the password provided shall be configured on the FortiSwitch against the default "admin" account already present.

Number of switches per FortiGate based on model (388024)

The maximum number of supported FortiSwitches depends on the FortiGate model:

FortiGate Model Range	Number of FortiSwitches Supported
Up to FortiGate-98 and FortiGate-VM01	8
FortiGate-100 to 280 and FortiGate-VM02	24
FortiGate-300 to 5*xx*	48
FortiGate-600 to 900 and FortiGate-VM04	64
FortiGate-1000 and up	128
FortiGate-3*xxx* and up, and FortiGate-VM08 and up	256

Miscellaneous configuration option changes

- The default value of `dhcp-snooping` (also called DHCP-blocking) is changed from `trusted` in FortiOS 5.4 to `untrusted` in FortiOS 5.6.
- The default value of `edge-port` is changed from `disabled` in FortiOS 5.4 to `enabled` in FortiOS 5.6.0.
- The default value for DHCP snooping on the FortiLink VLAN (system interface) is changed from “enabled” in FortiOS 5.6.2 and earlier to “disabled” in FortiOS 5.6.3 and later. Note that, in the GUI, DHCP snooping is automatically changed to “enable” when the DHCP server is enabled on the interface.

Additional GUI support

- Link aggregation of FortiSwitch ports
- DHCP trusted/untrusted, loop guard, and STP for FortiSwitch ports
- Connect to CLI support for FortiSwitch

What's new for managed FortiSwitches in FortiOS 5.6 with FortiSwitch 3.5.4 (and later releases)

This section describes new managed FortiSwitch features in FortiOS 5.6 with FortiSwitch 3.5.4.

Aggregating FortiSwitches into groups (397950)

In larger networks, the number of switches can be large. Different models and device purposes might exist. Furthermore, the topology might have "built-in" redundancy. Use the following command to create a FortiSwitch group allowing you to perform an operation on the entire group instead of one switch at a time.

```
config switch-controller switch-group
   edit <name>
      set description <string>
      set members <..> <..>
      end
   end
```

Pre-authentication and replacements of FortiSwitches (298533)

FortiSwitch configuration templates allow you to replace a FortiSwitch and have the configuration of the original FortSwitch installed on the replacement.

Use the `execute replace-device fortiswitch <sn-old> <sn-new>` to transfer the configuration for the FortiSwitch with serial number `<sn-old>` to the replacement FortiSwitch with serial number `<sn-new>`.

LLDP MED on managed FortiSwitches (372288)

FortiOS 5.6 supports configuring link layer discovery protocol-media endpoint discovery (LLDP MED) for managed FortiSwitches. Additionally, you can use FortiGate CLI commands display the information collected by LLDP on the FortiSwitch.

You can use the following command to add media endpoint discovery (MED) features to an LLDP profile.

```
config switch-controller lldp-profile
   edit <lldp-profle>
        config med-network-policy
           edit guest-voice
              set status {disable | enable}
           next
           edit guest-voice-signaling
              set status {disable | enable}
           next
           edit guest-voice-signaling
              set status {disable | enable}
```

```
            next
            edit softphone-voice
               set status {disable | enable}
            next
            edit streaming-video
               set status {disable | enable}
            next
            edit video-conferencing
               set status {disable | enable}
            next
            edit video-signaling
               set status {disable | enable}
            next
            edit voice
               set status {disable | enable}
            next
            edit voice-signaling
               set status {disable | enable}
            end
         config custom-tlvs
            edit <name>
               set oui <identifier>
               set subtype <subtype>
               set information-string <string>
            end
      end
```

Enhanced 802.1x including FortiSwitch port security policy framework (389102)

New FortiSwitch port security features include:

- Dynamic VLAN Assignment
- “guest” and “auth-fail” VLAN
- Mac Address Bypass (MAB)
- Multiple host support on single physical port

Global settings applied across the network

```
config switch-controller 802.1x-settings
   set reauth-period < int >
   set max-reauth-attempt < int >
   set link-down-auth < *set-unauth | no-action >
end
```

Local switch overrides

```
config switch-controller managed-switch
   edit < switch >
      config 802.1x-settings
         set local-override {disable | enable}
         set reauth-period <int>
         set max-reauth-attempt <int>
         set link-down-auth {set-unauth | no-action}
      end
```

```
   next
end
```

Policy definitions (802.1x and captive-portal)

```
config switch-controller security-policy 802.1x
   edit 8021X-policy-default
      set user-group <user.group>
      set mac-auth-bypas {disable | enable}
      set guest-vlan {disable | enable}
      set guest-vlanid <vlan-id>
      set guest-auth-delay <int>
      set auth-fail-vlan  {disable | enable}
      set auth-fail-vlanid <vlan-id>
      radius-timeout-overwrite {disable | enable}
   end
end


config switch-controller security-policy captive-portal
   edit captive-portal-default
      set vlan <vlan-id>
      config users
         edit 1
            set user-group <usergroup>
            set vlanid <vlan-id>
         next
      end
   end
end
```

Port settings

```
config switch-controller managed-switch
   edit <managed-switch>
      config ports
         edit <port>
            set port-security-policy {802.1x-policy | captive-portal-policy}
         next
      end
   next
end
```

Firmware upgrade management and compatible version information (385171)

You can view the current firmware version of a FortiSwitch and upgrade the FortiSwitch to a new firmware version by going to **WiFi & Switch Controller > Managed FortiSwitch** and editing one of the FortiSwitches. Under **Firmware** you can see the current firmware version and select **Update** to update it.

Changed managed-switch display format for 'dynamic-capability' (387239)

FortiOS 5.6.0 displays capability flags as strings such as: dynamic-capability, igmp-snooping, dhcp-snooping, and so on. For example:

```
config switch-controller managed-switch
edit S124DP3X15000315
get
switch-id : S124DP3X15000315
name :
description :
fsw-wan1-peer : port9
fsw-wan1-admin : enable
fsw-wan2-peer :
fsw-wan2-admin : discovered
directly-connected : 0
connected : 1
version : 1
pre-provisioned : 0
dynamic-capability : igmp-snooping,dhcp-snooping
switch-device-tag :
dynamically-discovered: 1
```

Connecting to a managed switch CLI from the FortiGate GUI (378119)

To connect to a FortiSwitch CLI, go to **WiFi & Switch Controller > Managed FortiSwitch**, right click on the FortiSwitch to connect to and select **Connect to CLI**. You can also open the FortiGate CLI console and use the `execute telnet <ip>` command, where `<ip>` is the management IP address of the FortiSwitch.

Firmware upgrade of stacked or tiered switches (355050)

From your FortiGate CLI, you can upgrade the firmware of all of the managed FortiSwitches of the same model using a single `execute` command. The command includes the name of a firmware image file and all of the managed FortiSwitches compatible with that firmware image file are upgraded. For example:

```
execute switch-controller stage-tiered-swtp-image ALL <firmware-image-file>
```

You can also use the following new command to restart all of the managed FortiSwitches after a 2-minute delay.

```
execute switch-controller restart-swtp-delayed ALL
```

More information displayed by the execute switch-controller get-conn-status command (388751)

The `get-conn-status` command now displays more information for each managed switch including the ID of each switch, the version of the firmware running on the switch, the status of the switch, the IP address for managing the switch, and its join time.

```
execute switch-controller get-conn-status
Managed-devices in current vdom root:

STACK-NAME: FortiSwitch-Stack-port3
```

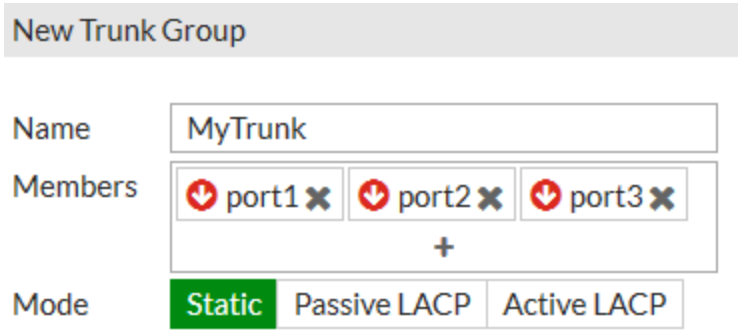
```
SWITCH-ID         VERSION  STATUS           ADDRESS     JOIN-TIME NAME
FS108D3W16001177 v3.4     Authorized/Down 169.254.1.2 N/A       My-Switch
```

User-port link aggregation groups available on the GUI (378470)

The GUI now supports the ability to configure user port LAGs on managed FortiSwitches.

To create a link aggregation group for FortiSwitch user ports:

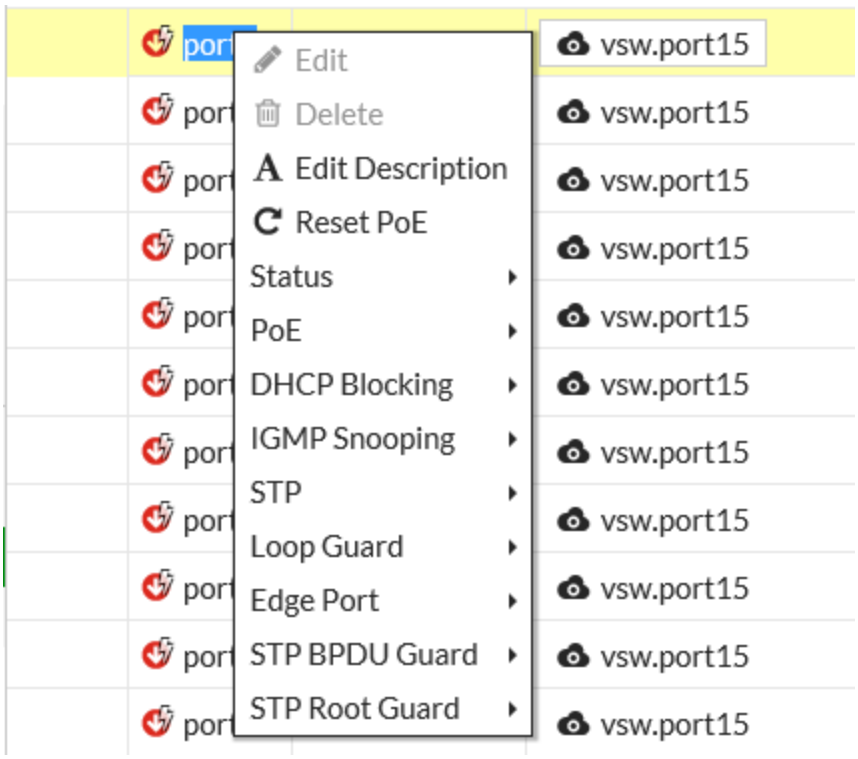
1. Go to **WiFi & Switch Controller > FortiSwitch Ports**.
2. Click **Create New > Trunk**.
3. In the New Trunk Group page enter a **Name** for the trunk group.
4. Select two or more physical ports to add to the trunk group.
5. Select the **Mode**: Static, Passive LACP, or Active LACP.
6. Click OK.



DHCP blocking, STP, and loop guard on managed FortiSwitch ports on the GUI (375860)

The managed FortiSwitch GUI now supports the ability to enable/disable DHCP blocking, STP and loop guard for FortiSwitch user ports.

Go to **WiFi & Switch Controller > FortiSwitch Ports**. For any port you can select DHCP Blocking, STP, or Loop Guard. STP is enabled on all ports by default. Loop guard is disabled by default on all ports.



New switch profiles (387398)

Switch profiles allow specific settings to be applied to all authorized FortiSwitches. The default switch profile is automatically bound to every switch discovered by the FortiGate. You can create additional profiles as needed.

Within a switch profile, you can control the behavior of the FortiSwitch's admin account.You can add a password to a profile or create a new profile and bind that profile to any switch. The password provided in the profile is configured on the FortiSwitch to the default admin administrator account.

Miscellaneous configuration option changes

- On a switch port, the default value of `dhcp-snooping` (also called DHCP-blocking) is changed from `trusted` in FortiOS 5.4 to `untrusted` in FortiOS 5.6.
- On a switch port, the default value of STP `edge-port` is changed from `disabled` in FortiOS 5.4 to `enabled` in FortiOS 5.6.0.
- The default value of `fortilink-split-port` is changed from `disable` in FortiOS 5.4.1/5.4.2 to `enable` in FortiOS 5.4.3 onward. This command applies to FortiGate aggregate interfaces.

```
config system interface
   edit <name of the FortiLink interface>
      set fortilink-split-interface enable
   end
```

- The default value for DHCP snooping on the FortiLink VLAN (system interface) is changed from "enabled" in FortiOS 5.6.2 and earlier to "disabled" in FortiOS 5.6.3 and later. Note that, in the GUI, DHCP snooping is automatically changed to "enable" when the DHCP server is enabled on the interface.

Before you begin

Before you configure the managed FortiSwitch unit, the following assumptions have been made in the writing of this manual:

- You have completed the initial configuration of the FortiSwitch unit, as outlined in the QuickStart Guide for your FortiSwitch, and you have administrative access to the FortiSwitch Web-based manager and CLI.
- You have installed a FortiGate unit on your network and have administrative access to the FortiGate Web-based manager and CLI.

How this guide is organized

This guide contains the following sections:

- Connecting FortiLink ports - information about connecting FortiSwitch ports to FortiGate ports.
- FortiLink configuration using the FortiGate GUI
- FortiLink configuration using the FortiGate CLI
- Network topologies for managed FortiSwitches - describes the configuration for various stacking topologies.
- Optional setup tasks - describes other setup tasks.
- FortiSwitch features configuration - describes configuring managed FortiSwitch features including VLANs.
- FortiSwitch port features - configure ports and PoE from the FortiGate unit.
- FortiSwitch port security policy - describes setting up FortiSwitch security policies.
- Additional capabilities - describes extra FortiSwitch features.
- Troubleshooting - describes techniques for troubleshooting common problems.

Connecting FortiLink ports

This section contains information about the FortiSwitch and FortiGate ports that you connect to establish a FortiLink connection.

For all FortiGate models, you can connect up to 16 FortiSwitches to one FortiGate unit.

In FortiSwitchOS 3.3.0 and later releases, you can use any of the switch ports for FortiLink. Some or all of the switch ports (depending on the model) support auto-discovery of the FortiLink ports.

You can chose to connect a single FortiLink port or multiple FortiLink ports as a logical interface (link-aggregation group, hardware switch, or software switch).

1. Enable the switch controller on FortiGate

Before connecting the FortiSwitch and FortiGate units, ensure that the switch controller feature is enabled on the FortiGate with the FortiGate Web-based manager or CLI to enable the switch controller. Depending on the FortiGate model and software release, this feature may be enabled by default.

Using the FortiGate GUI

1. Go to **System > Feature Visibility**.
2. Turn on the **Switch Controller** feature, which is in the **Basic Features** list.
3. Select **Apply**.

The menu option **WiFi & Switch Controller** now appears.

Using the FortiGate CLI

Use the following commands to enable the Switch Controller:

```
config system global
   set switch-controller enable
end
```

2. Connect the FortiSwitch and FortiGate

FortiSwitchOS 3.3.0 and later provides flexibility for FortiLink:

- Use any switch port for FortiLink
- Provides auto-discovery of the FortiLink ports on the FortiSwitch
- Choice of a single FortiLink port or multiple FortiLink ports in a link-aggregation group (LAG)

Auto-discovery of the FortiSwitch ports

In FortiSwitchOS 3.3.0 and later releases, D-series FortiSwitch models support FortiLink auto-discovery, on automatic detection of the port connected to the FortiGate.

You can use any of the switch ports for FortiLink. Before connecting the switch to the FortiGate, use the following FortiSwitch CLI commands to configure a port for FortiLink auto-discovery:

```
config switch interface
   edit <port>
   set auto-discovery-fortilink enable
end
```

By default, each FortiSwitch model provides a set of ports that are enabled for FortiLink auto-discovery. If you connect the FortiLink using one of these ports, no switch configuration is required.

In FortiSwitchOS 3.4.0 and later releases, the last four ports are the default auto-discovery FortiLink ports. You can also run the **show switch interface** command on the FortiSwitch to see the ports that have auto-discovery enabled.

The following table lists the default auto-discovery ports for each switch model. **NOTE:** Any port can be used for FortiLink if it is manually configured.

FortiSwitch Model	Default Auto-FortiLink ports
FS-108D	ports 9 and 10
FS-108D-POE	ports 9 and 10
FSR-112D	ports 9, 10, 11 and 12
FSR-112D-POE	ports 5, 6, 7, 8, 9, 10, 11, and 12
FS-124D, FS-124D-POE	ports 23, 24, 25, and 26
FS-224D-POE	ports 21, 22, 23, and 24
FS-224D-FPOE	ports 21, 22, 23, 24, 25, 26, 27, and 28
FS-248D, FS-248D-FPOE, FS-448D, FS-448D-FPOE, FS-448D-POE	ports 45, 46, 47, 48, 49, 50, 51, and 52
FS-248D-POE	ports 47, 48, 49, and 50
FS-424D, FS-424D-POE, FS-424D-FPOE	ports 23, 24, 25, and 26
FS-524D, FS-524D-FPOE	ports 21, 22, 23, 24, 25, 26, 27, 28, 29, and 30
FS-548D, FS-548D-FPOE	ports 45, 46, 47, 48, 49, 50, 51, 52, 53, and 54
FS-1024D, FS-1048D, FS-3032D	all ports

Choosing the FortiGate ports

The FortiGate manages all of the switches through one active FortiLink. The FortiLink may consist of one port or multiple ports (for a LAG).

As a general rule, FortiLink is supported on all ports that are not listed as HA ports.

FortiLink configuration using the FortiGate GUI

This section describes how to configure a FortiLink between a FortiSwitch and a FortiGate.

You can configure FortiLink using the FortiGate GUI or CLI. Fortinet recommends using the GUI because the CLI procedures are more complex (and therefore more prone to error).

If you use one of the auto-discovery FortiSwitch ports, you can establish the FortiLink connection (single port or LAG) with no configuration steps on the FortiSwitch and with a few simple configuration steps on the FortiGate.

Summary of the procedure

1. On the FortiGate, configure the FortLink port or create a logical FortLink interface.
2. Authorize the managed FortiSwitch.

Configure FortiLink as a single link

To configure the FortiLink port on the FortiGate:

1. Go to **Network** > **Interfaces**.
2. (Optional) If the FortiLink physical port is currently included in the internal interface, edit it and remove the desired port from the Physical Interface Members.
3. Edit the FortiLink port.
4. Set **Addressing mode** to **Dedicated to FortiSwitch**.
5. Configure the **IP/Network Mask** for your network.
6. Optionally select **Automatically authorize devices** or disable to manually authorize the FortiSwitch.
7. Select **OK**.

Configure FortiLink as a logical interface

You can configure the FortiLink as a logical interface: link-aggregation group (LAG), hardware switch, or software switch).

LAG is supported on all FortiSwitch models and on FortiGate models FGT-100D and above. Hardware switch is supported on some FortiGate models.

Connect any of the FortiLink-capable ports on the FortiGate to the FortiSwitch. Ensure that you configure auto-discovery on the FortiSwitch ports (unless it is so by default).

1. Go to **Network > Interfaces**.
2. (Optional) If the FortiLink physical ports are currently included in the internal interface, edit the internal interface, and remove the desired ports from the Physical Interface Members.
3. Select **Create New > Interface**.
4. Enter a name for the interface (11 characters maximum).
5. Set the **Type** to **802.3ad Aggregate, Hardware Switch**, or **Software Switch**.
6. Select the FortiGate ports for the logical interface.

7. Set **Addressing mode** to **Dedicated to FortiSwitch**.
8. Configure the **IP/Network Mask** for your network.
9. Optionally select **Automatically authorize devices** or disable to manually authorize the FortiSwitch.
10. Select **OK**.

FortiLink split interface

You can use the FortiLink split interface to connect the FortiLink aggregate interface from one FortiGate to two FortiSwitches. When the FortiLink split interface is enabled, only one link remains active.

The aggregate interface for this configuration must contain exactly two physical ports (one for each FortiSwitch).

You must enable the split interface on the FortiLink aggregate interface using the FortiGate CLI:

```
config system interface
   edit <name of the FortiLink interface>
      set fortilink-split-interface enable
end
```

Authorizing the FortiSwitch

If you configured the FortiLink interface to manually authorize the FortiSwitch as a managed switch, perform the following steps:

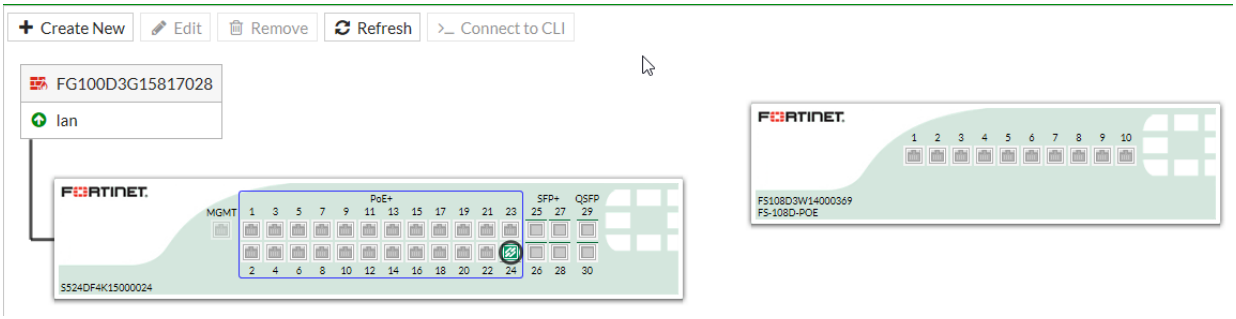
1. Go to **WiFi & Switch Controller** > **Managed FortiSwitch**.
2. Optionally, click on the FortiSwitch faceplate and click **Authorize**. This step is required only if you disabled the automatic authorization field of the interface.

Adding preauthorized FortiSwitches

After you preauthorize a FortiSwitch, you can assign the FortiSwitch ports to a VLAN.

To preauthorize a FortiSwitch:

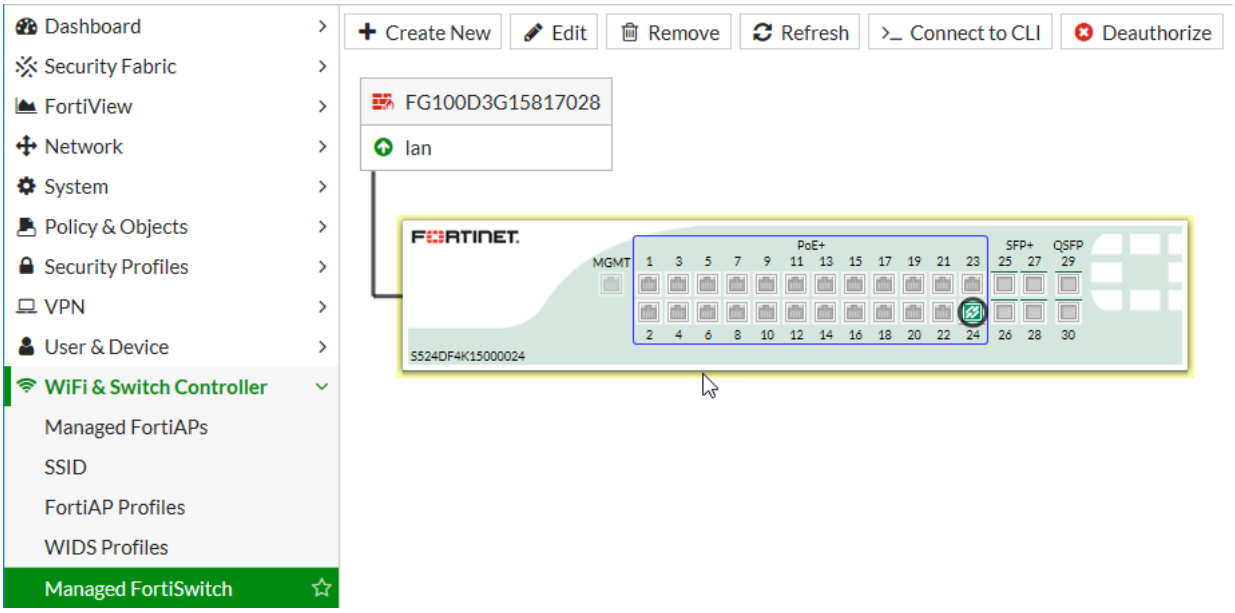
1. Go to **WiFi & Switch Controller** > **Managed FortiSwitch**.
2. Click **Create New**.
3. In the New Managed FortiSwitch page, enter the serial number, model name, and description of the FortiSwitch.
4. Move the **Authorized** slider to the right.
5. Click **OK**.
   The Managed FortiSwitch page shows a FortiSwitch faceplate for the preauthorized switch.



Managed FortiSwitch display

Go to **WiFi & Switch Controller** > **Managed FortiSwitch** to see all of the switches being managed by your FortiGate.

When the FortiLink is established successfully, the status is green (next to the FortiGate interface name and on the FortiSwitch faceplate), and the link between the ports is a solid line.



If the link has gone down for some reason, the line will be dashed, and a broken link icon will appear. You can still edit the FortiSwitch though and find more information about the status of the switch. The link to the FortiSwitch may be down for a number of reasons; for example, a problem with the cable linking the two devices, firmware versions being out of synch, and so on. You need to make sure the firmware running on the FortiSwitch is compatible with the firmware running on the FortiGate.

From the Managed FortiSwitch page, you can edit any of the managed FortiSwitches, remove a FortiSwitch from the configuration, refresh the display, connect to the CLI of a FortiSwitch, or deauthorize a FortiSwitch.

Edit a managed FortiSwitch

To edit a managed FortiSwitch:

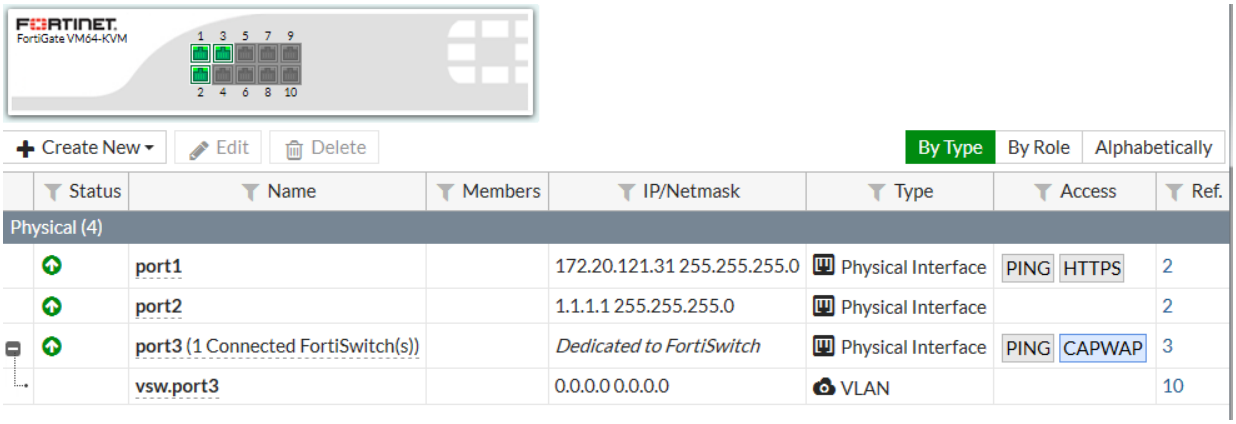
1. Go to **WiFi & Switch Controller > Managed FortiSwitch**.
2. Click on the FortiSwitch to and click **Edit**, right-click on a FortiSwitch and select **Edit**, or double-click on a FortiSwitch.

From the **Edit Managed FortiSwitch** form, you can:

- Change the **Name** and **Description** of the FortiSwitch.
- View the **Status** of the FortiSwitch.
- **Restart** the FortiSwitch.
- **Authorize** or deauthorize the FortiSwitch.
- **Update** the firmware running on the switch.

Network interface display

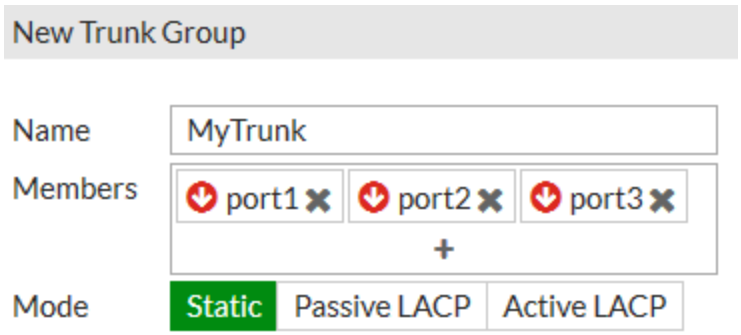
On the **Network > Interfaces** page, you can see the FortiGate interface connected to the FortiSwitch. The GUI indicates **Dedicated to FortiSwitch** in the IP/Netmask field.



Add link aggregation groups (Trunks)

To create a link aggregation group for FortiSwitch user ports:

1. Go to **WiFi & Switch Controller > FortiSwitch Ports**.
2. Click **Create New > Trunk**.
3. In the New Trunk Group page, enter a **Name** for the trunk group.
4. Select two or more physical ports to add to the trunk group.
5. Select the **Mode**: Static, Passive LACP, or Active LACP.
6. Click **OK**.

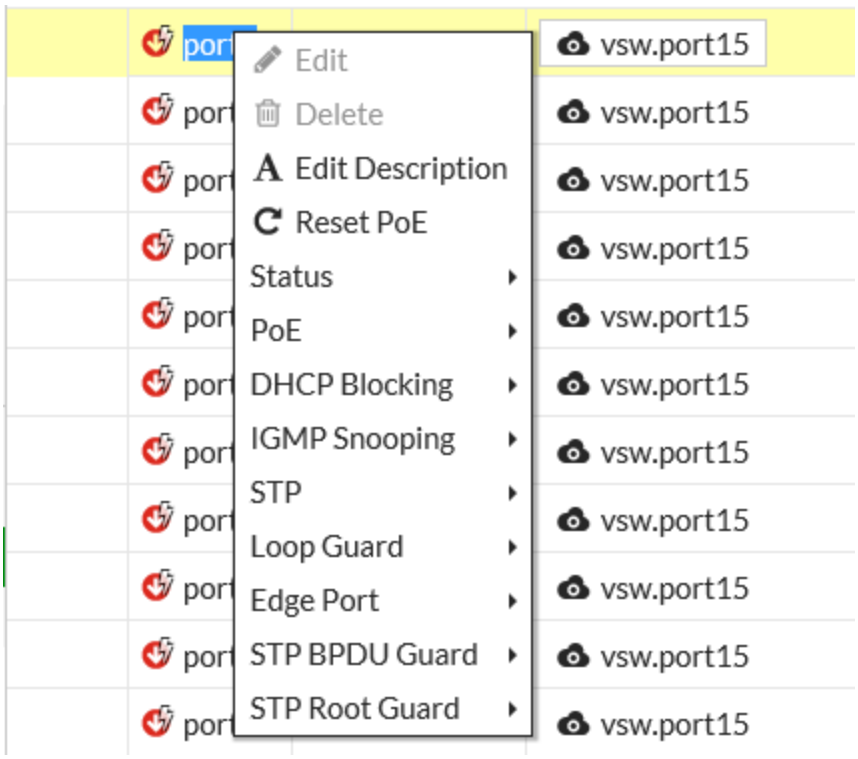


Configure DHCP blocking, IGMP snooping, STP, and loop guard on managed FortiSwitch ports

Go to **WiFi & Switch Controller > FortiSwitch Ports**. Right-click any port and then enable or disable the following features:

- **DHCP blocking**—The DHCP blocking feature monitors the DHCP traffic from untrusted sources (for example, typically host ports and unknown DHCP servers) that might initiate traffic attacks or other hostile actions. To prevent this, DHCP blocking filters messages on untrusted ports.
- **IGMP snooping**—IGMP snooping allows the FortiSwitch to passively listen to the Internet Group Management Protocol (IGMP) network traffic between hosts and routers. The switch uses this information to determine which ports are interested in receiving each multicast feed. FortiSwitch can reduce unnecessary multicast traffic on the LAN by pruning multicast traffic from links that do not contain a multicast listener.
- **Spanning Tree Protocol (STP)**—STP is a link-management protocol that ensures a loop-free layer-2 network topology.
- **Loop guard**—A loop in a layer-2 network results in broadcast storms that have far-reaching and unwanted effects. Fortinet loop guard helps to prevent loops. When loop guard is enabled on a switch port, the port monitors its subtending network for any downstream loops. The loop guard feature is designed to work in concert with STP rather than as a replacement for STP.
- **STP root guard**—Root guard protects the interface on which it is enabled from becoming the path to root. When enabled on an interface, superior BPDUs received on that interface are ignored or dropped. Without using root guard, any switch that participates in STP maintains the ability to reroute the path to root. Rerouting might cause your network to transmit large amounts of traffic across suboptimal links or allow a malicious or misconfigured device to pose a security risk by passing core traffic through an insecure device for packet capture or inspection. By enabling root guard on multiple interfaces, you can create a perimeter around your existing paths to root to enforce the specified network topology.
- **STP BPDU guard**—Similar to root guard, BPDU guard protects the designed network topology. When BPDU guard is enabled on STP edge ports, any BPDUs received cause the ports to go down for a specified number of minutes. The BPDUs are not forwarded, and the network edge is enforced.

STP is enabled on all ports by default. Loop guard is disabled by default on all ports.


Edit
Delete
Edit Description
Reset PoE
Status
PoE
DHCP Blocking
IGMP Snooping
STP
Loop Guard
Edge Port
STP BPDU Guard
STP Root Guard
vsw.port15

FortiLink configuration using the FortiGate CLI

This section describes how to configure FortiLink using the FortiGate CLI. Fortinet recommends using the FortiGate GUI because the CLI procedures are more complex (and therefore more prone to error).

If you use one of the auto-discovery FortiSwitch ports, you can establish the FortiLink connection (single port or LAG) with no configuration steps on the FortiSwitch and with a few simple configuration steps on the FortiGate.

Summary of the procedure

1. Remove the port(s) from the LAN interface.
2. Configure the FortLink port or create a logical FortLink interface if it is required on the model you are using.
3. Configure NTP.
4. Authorize the managed FortiSwitch.
5. Configure DHCP.

Configure FortiLink as a single link

Configure the FortiLink port on the FortiGate and authorize the FortiSwitch as a managed switch.

In the following steps, port 1 is configured as the FortiLink port.

1. If required, remove port 1 from the **lan** interface:
```
config system virtual-switch
   edit lan
      config port
         delete port1
      end
   end
end
```
2. Configure port 1 as the FortiLink interface:
```
config system interface
   edit port1
      set auto-auth-extension-device enable
      set fortilink enable
   end
end
```
3. Configure an NTP server on port 1:
```
config system ntp
   set server-mode enable
   set interface port1
end
```
4. Authorize the FortiSwitch unit as a managed switch.
```
config switch-controller managed-switch
```

```
   edit FS224D3W14000370
      set fsw-wan1-admin enable
   end
end
```

NOTE: FortiSwitch will reboot when you issue the **set fsw-wan1-admin enable** command.

Configure FortiLink as a logical interface

You can configure the FortiLink as a logical interface: link-aggregation group (LAG), hardware switch, or software switch).

NOTE: LAG is supported on all FortiSwitch models and on FortiGate models FGT-100D and above. Hardware switch is supported on some FortiGate models.

Connect any of the FortiLink-capable ports on the FortiGate to the FortiSwitch. Ensure that you configure auto-discovery on the FortiSwitch ports (unless it is auto-discovery by default).

In the following procedure, port 4 and port 5 are configured as a FortiLink LAG.

1. If required, remove the FortiLink ports from the **lan** interface:

```
config system virtual-switch
   edit lan
      config port
         delete port4
         delete port5
      end
   end
end
```

2. Create a trunk with the two ports that you connected to the switch:

```
config system interface
   edit flink1 (enter a name, 11 characters maximum)
      set allowaccess ping capwap https
      set vlanforward enable
      set type aggregate
      set member port4 port5
      set lacp-mode static
      set fortilink enable
      (optional) set fortilink-split-interface enable
   next
end
```

NOTE: If the members of the aggregate interface connect to more than one FortiSwitch, you must enable **fortilink-split-interface**.

3. Authorize the FortiSwitch unit as a managed switch.

```
config switch-controller managed-switch
   edit FS224D3W14000370
      set fsw-wan1-admin enable
   end
end
```

NOTE: FortiSwitch will reboot when you issue the **set fsw-wan1-admin enable** command.

Network topologies for managed FortiSwitches

The FortiGate requires only one active FortiLink to manage all of the subtending FortiSwitches (called *stacking*).

You can configure the FortiLink as a physical interface or as a logical interface (associated with one or more physical interfaces). Depending on the network topology, you may also configure a standby FortiLink.

For any of the topologies, note the following:

- All of the managed FortiSwitches will function as one Layer-2 stack where the FortiGate manages each FortiSwitch separately.
- The active FortiLink carries data as well as management traffic.

Supported topologies

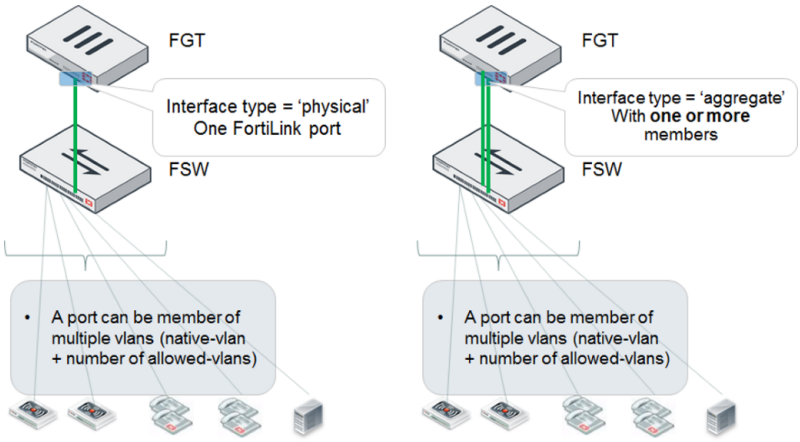
Fortinet recommends the following topologies for managed FortiSwitches:

- Single FortiGate managing a single FortiSwitch
- Single FortiGate managing a stack of several FortiSwitches
- HA-mode FortiGates managing a single FortiSwitch
- HA-mode FortiGates managing a stack of several FortiSwitches
- HA-mode FortiGates managing a FortiSwitch two-tier topology
- Single FortiGate managing multiple FortiSwitches (using a hardware or software switch interface)
- HA-mode FortiGates managing two-tier FortiSwitches with access rings
- Dual-homed servers connected to FortiLink tier-1 FortiSwitches using an MCLAG
- Standalone FortiGate with dual-homed FortiSwitch access
- HA-mode FortiGates with dual-homed FortiSwitch access

Single FortiGate managing a single FortiSwitch

On the FortiGate, the FortiLink interface is configured as physical or aggregate. The 802.3ad aggregate interface type provides a logical grouping of one or more physical interfaces.

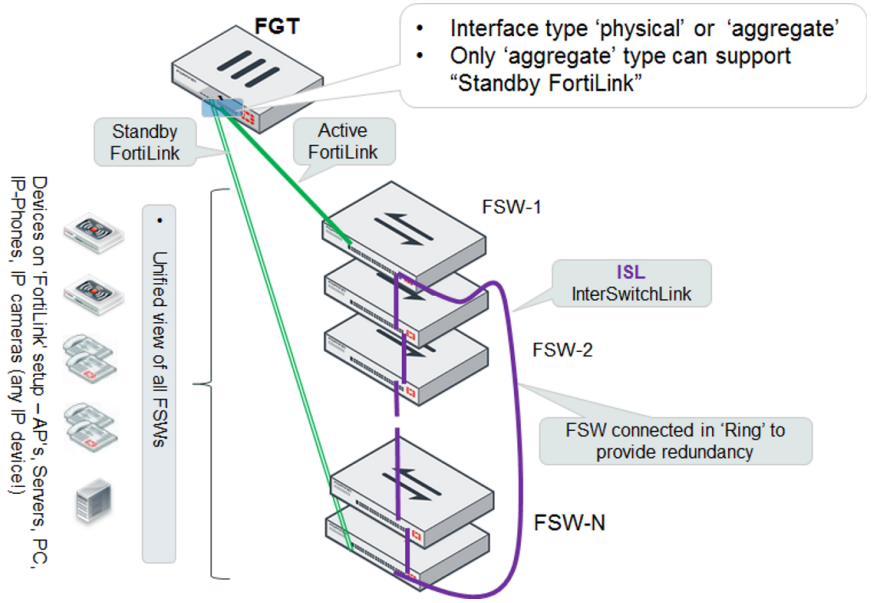
NOTE: For the aggregate interface, you must disable the split interface on the FortiGate.



Single FortiGate managing a stack of several FortiSwitches

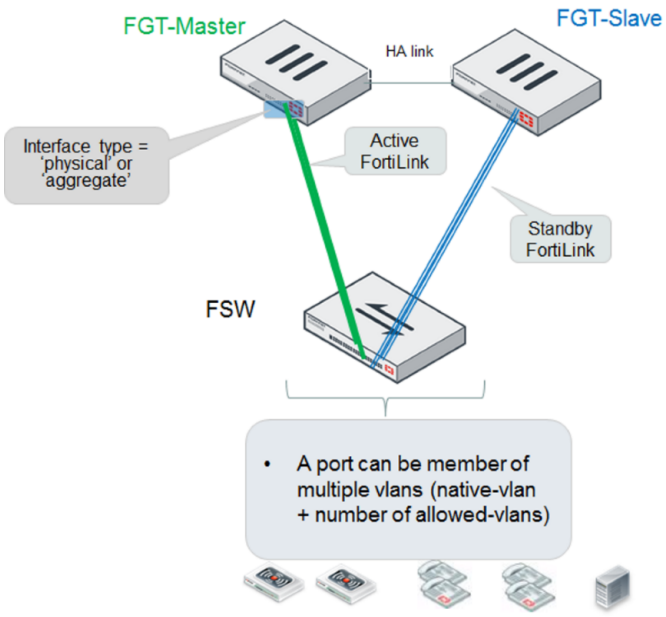
The FortiGate connects directly to one FortiSwitch device using a physical or aggregate interface. The remaining FortiSwitches connect in a ring using inter-switch links (that is, ISL).

Optionally, you can connect a standby FortiLink connection to the last FortiSwitch. For this configuration, you create a FortiLink Split-Interface (an aggregate interface that contains one active link and one standby link).



HA-mode FortiGates managing a single FortiSwitch

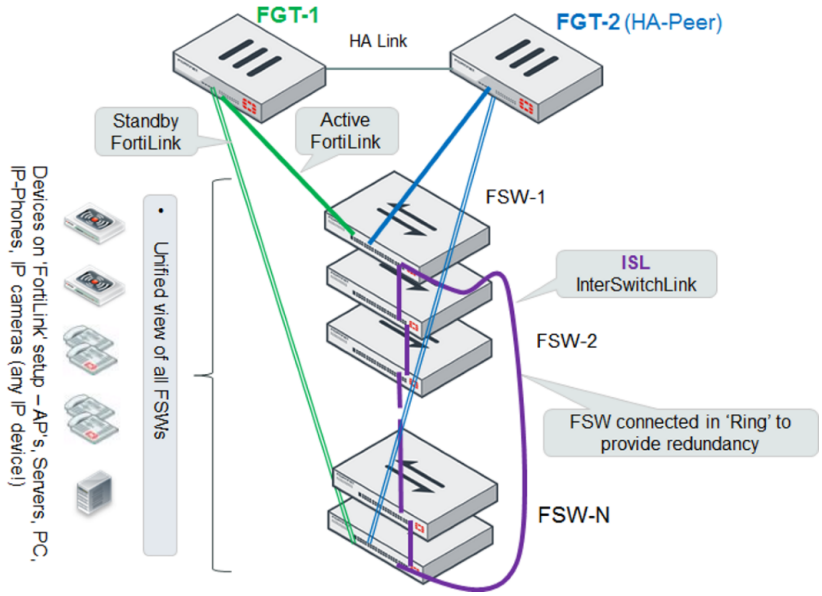
The master and slave FortiGate units both connect a FortiLink to the FortiSwitch. The FortiLink port(s) and interface type must match on the two FortiGate units.



HA-mode FortiGates managing a stack of several FortiSwitches

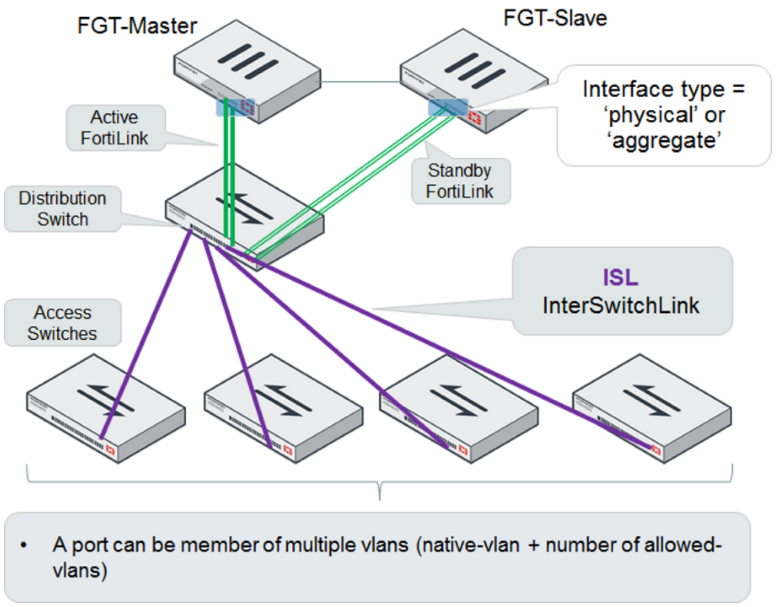
The master and slave FortiGate units both connect a FortiLink to the first FortiSwitch and (optionally) to the last FortiSwitch. The FortiLink ports and interface type must match on the two FortiGate units.

For the active/standby FortiLink configuration, you create a FortiLink Split-Interface (an aggregate interface that contains one active link and one standby link).



HA-mode FortiGates managing a FortiSwitch two-tier topology

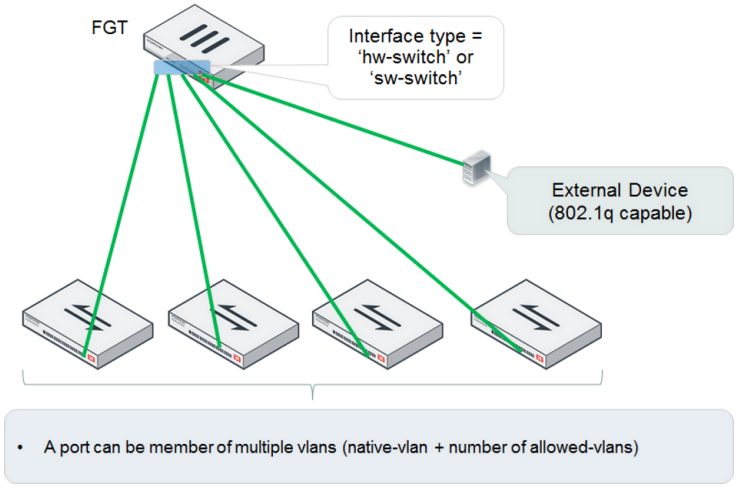
The distribution FortiSwitch connects to the master and slave FortiGate units. The FortiLink port(s) and interface type must match on the two FortiGate units.



Single FortiGate managing multiple FortiSwitches (using a hardware or software switch interface)

The FortiGate connects directly to each FortiSwitch. Each of these FortiLink ports is added to the logical hardware-switch or software-switch interface on the FortiGate.

Optionally, you can connect other devices to the FortiGate logical interface. These devices, which must support IEEE 802.1q VLAN tagging, will have Layer 2 connectivity with the FortiSwitch ports.



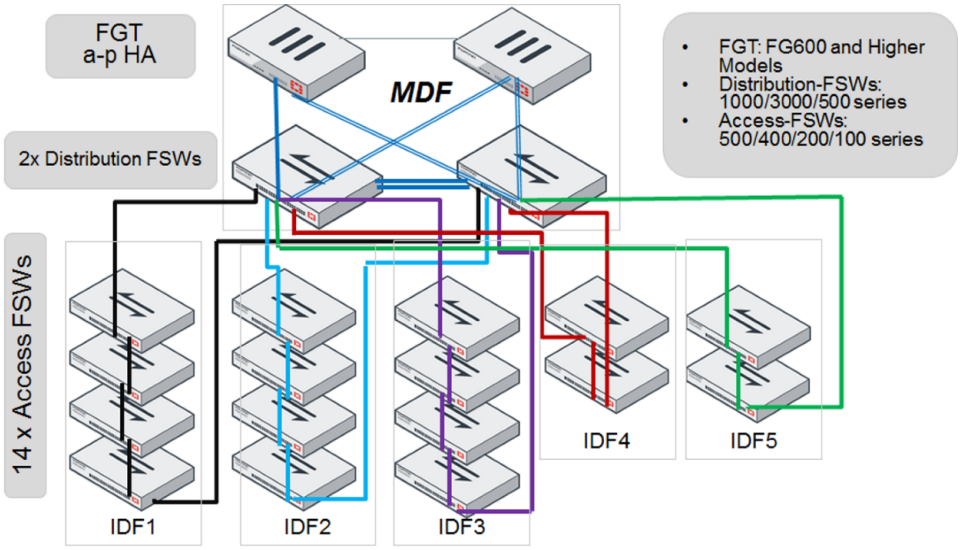
NOTE: Using the hardware or software switch interface in FortiLink mode is not recommended in most cases. It can be used when the traffic on the ports is very light because all traffic across the switches moves through FortiGate.

HA-mode FortiGates managing two-tier FortiSwitches with access rings

NOTE: MCLAG is not supported when access rings are present.

HA-mode FortiGates connect to redundant distribution FortiSwitches. Access FortiSwitches are arranged in a stack in each IDF, connected to both distribution switches.

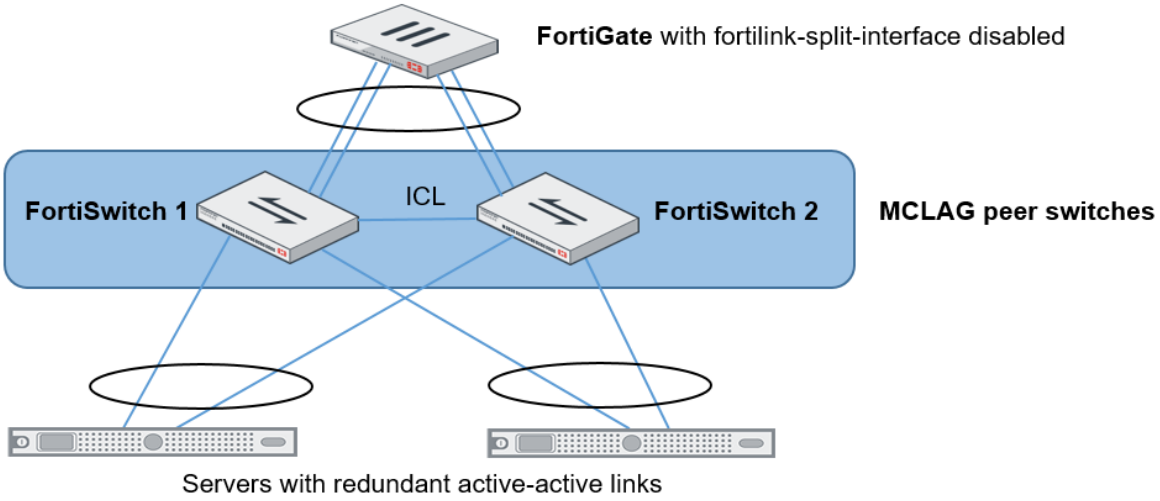
For the FortiLink connection to each distribution switch, you create a FortiLink split interface (an aggregate interface that contains one active link and one standby link).



Dual-homed servers connected to FortiLink tier-1 FortiSwitches using an MCLAG

To configure a multichassis LAG, you need to configure FortiSwitch 1 and FortiSwitch 2 as MCLAG peer switches before creating a two-port LAG. Use the `set mclag-icl enable` command to create an inter-chassis link (ICL) on each FortiSwitch. Then you set up two MCLAGs towards the servers, each MCLAG using one port from each FortiSwitch. You must disable the FortiLink split interface for the FortiGate.

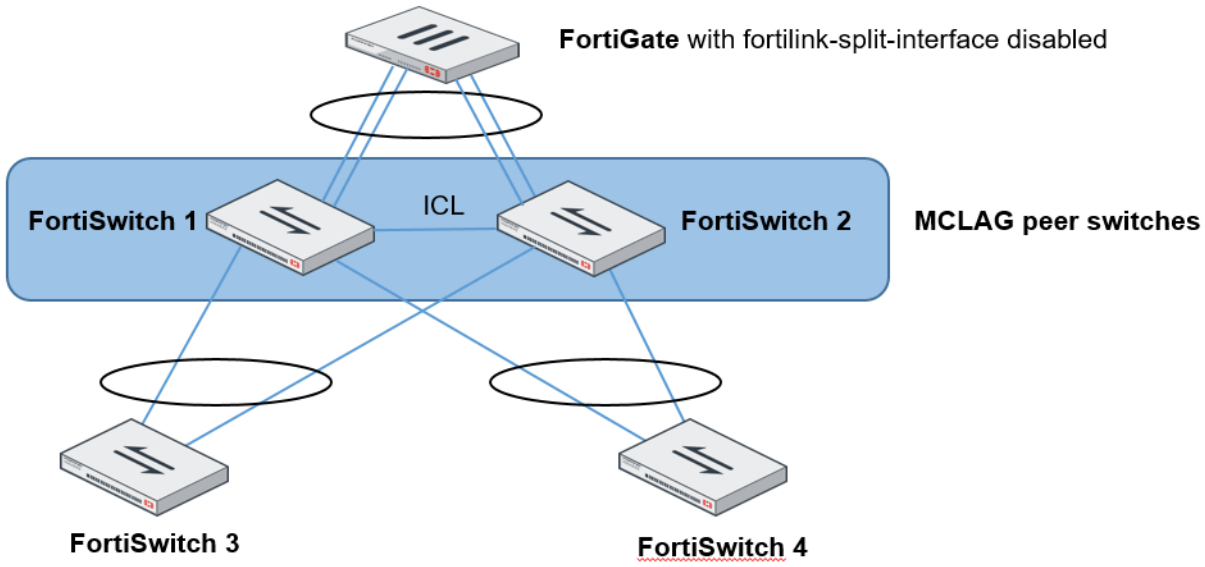
This topology is supported when the FortiGate is in HA mode.



Standalone FortiGate with dual-homed FortiSwitch access

This network topology provides high port density with two tiers of FortiSwitches.

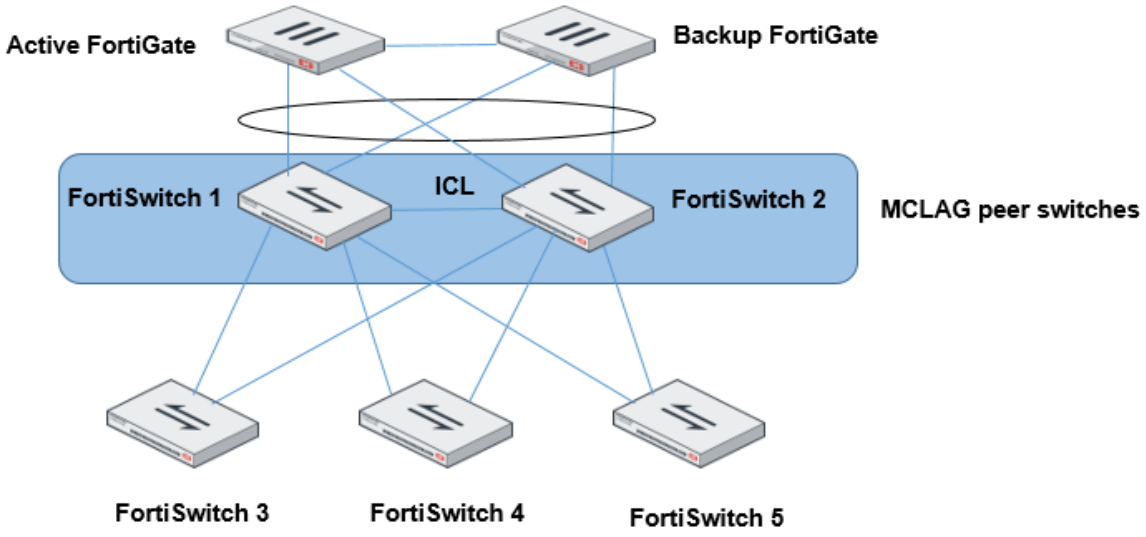
Use the `set mclag-icl enable` command to create an ICL on each FortiSwitch.



HA-mode FortiGates with dual-homed FortiSwitch access

In HA mode, only one FortiGate is active at a time. If the active FortiGate fails, the backup FortiGate becomes active.

Use the `set mclag-icl enable` command to create an ICL on each FortiSwitch.



Grouping FortiSwitches

You can simplify the configuration and management of complex topologies by creating FortiSwitch groups. A group can include one or more FortiSwitches and you can include different models in a group.

```
config switch-controller switch-group
   edit <name>
      set description <string>
      set members <serial-number> <serial-number> ...
      end
   end
```

Grouping FortiSwitches allows you to restart all of the switches in the group instead of individually. For example, you can use the following command to restart all of the FortiSwitches in a group named `my-sw-group`:

```
execute switch-controller restart-swtp my-switch-group
```

Upgrading the firmware of FortiSwitch groups is easier, too, because fewer commands are needed. See Firmware upgrade of stacked or tiered FortiSwitches on page 51.

Stacking configuration

To set up stacking:

1. Configure the active FortiLink interface on the FortiGate.
2. (Optional) Configure the standby FortiLink interface.
3. Connect the FortiSwitches together, based on your chosen topology.

1. Configure the active FortiLink

Configure the FortiLink interface (as described in the FortiLink configuration using the FortiGate GUI chapter).

When you configure the FortiLink interface, the stacking capability is enabled automatically.

2. Configure the standby FortiLink

Configure the standby FortiLink interface. Depending on your configuration, the standby FortiLink might connect to the same FortiGate as the active FortiLink or to a different FortiGate.

If the FortiGate receives discovery requests from two FortiSwitches, the link from one FortiSwitch will be selected as active, and the link from other FortiSwitch will be selected as standby.

If the active FortiLink fails, FortiGate converts the standby FortiLink to active.

3. Connect the FortiSwitches

Refer to the topology diagrams to see how to connect the FortiSwitches.

Inter-switch links (ISLs) form automatically between the stacked switches.

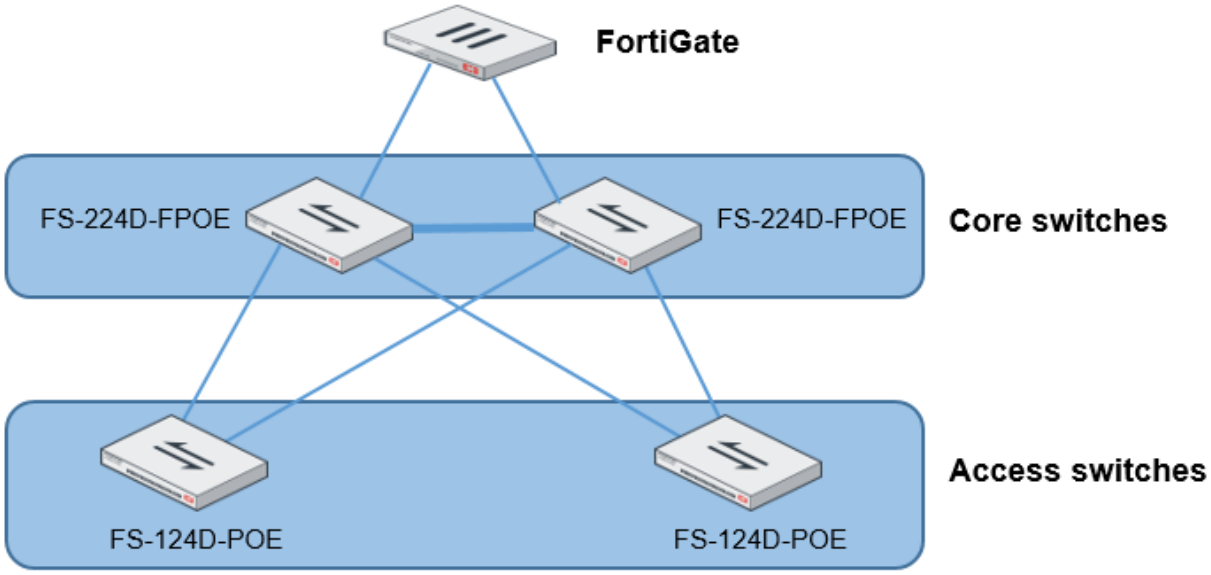
FortiGate will discover and authorize all of the FortiSwitches that are connected. After this, the FortiGate is ready to manage all of the authorized FortiSwitches.

Disable stacking

To disable stacking, execute the following commands from the FortiGate CLI. In the following example, port4 is the FortiLink interface:

```
config system interface
   edit port4
      set fortilink-stacking disable
   end
end
```

Firmware upgrade of stacked or tiered FortiSwitches



In this topology, the core FortiSwitches are model FS-224D-FPOE, and the access FortiSwitches are model FS-124D-POE. Because the switches are stacked or tiered, the procedure to update the firmware is simpler. In the following procedure, the four FortiSwitches are upgraded from 3.6.1 to 3.6.2.

To upgrade the firmware of stacked or tiered FortiSwitches:

1. Check that all of the FortiSwitches are connected and which firmware versions they are running. For example:

```
FG100E4Q16004478 (root) # execute switch-controller get-conn-status
Managed-devices in current vdom root:

STACK-NAME: FortiSwitch-Stack-flink
SWITCH-ID        VERSION    STATUS           ADDRESS         JOIN-TIME
NAME
S124DP3X15000118 v3.6.1     Authorized/Up    169.254.1.5     Mon Oct  2 14:06:08 2017     -
S124DP3X15000380 v3.6.1     Authorized/Up    169.254.1.4     Mon Oct  2 14:05:26 2017     -
S224DF3X16001718 v3.6.1     Authorized/Up    169.254.1.3     Mon Oct  2 14:05:37 2017     -
S224DF3X17000238 v3.6.1     Authorized/Up    169.254.1.2     Mon Oct  2 14:06:22 2017     -
```

2. Upload the firmware image for each FortiSwitch model (FS-224D-FPOE and FS-124D-POE) from either an FTP or TFTP server. If you are using a virtual domain (VDOM), you must enter the `config global` command before entering the `upload-swtp-image` command. For example:

```
FG100E4Q16004478 (global) # execute switch-controller upload-swtp-image tftp FSW_124D_POE-
v3-build0382-FORTINET.out 172.30.12.18

Downloading file FSW_124D_POE-v3-build0382-FORTINET.out from tftp server 172.30.12.18...
##################
Image checking ...
Image MD5 calculating ...
Image Saving S124DP-IMG.swtp ...
Successful!

File Syncing...

FG100E4Q16004478 (global) # execute switch-controller upload-swtp-image tftp FSW_224D_FPOE-
v3-build0382-FORTINET.out 172.30.12.18

Downloading file FSW_224D_FPOE-v3-build0382-FORTINET.out from tftp server 172.30.12.18...
####################
Image checking ...
Image MD5 calculating ...
Image Saving S224DF-IMG.swtp ...
Successful!

File Syncing...
```

3. Check which firmware images are available. For example:

```
FG100E4Q16004478 (root) # execute switch-controller list-swtp-image
SWTP Images on AC:
ImageName              ImageSize(B)    ImageInfo             ImageMTime
S124DP-IMG.swtp        19174985        S124DP-v3.6-build382  Mon Oct  2 14:40:54 2017
S224DF-IMG.swtp        23277106        S224DF-v3.6-build382  Mon Oct  2 14:42:55 2017
```

4. Stage the firmware image for each FortiSwitch model (FS-224D-FPOE and FS-124D-POE). For example:

```
FG100E4Q16004478 (root) # execute switch-controller stage-tiered-swtp-image ALL S124DP-
IMG.swtp
Staged Image Version S124DP-v3.6-build382

FG100E4Q16004478 (root) # execute switch-controller stage-tiered-swtp-image ALL S224DF-
IMG.swtp
Staged Image Version S224DF-v3.6-build382
```

5. Check that the correct firmware image is staged for each FortiSwitch. For example:

```
FG100E4Q16004478 (root) # diagnose switch-controller dump network-upgrade status
Device                                                          State

================================================================================================
================================
VDOM : root
S224DF3X16001718                        Running : S224DF-v3.6.1-build372,170620 (GA)
Next Boot : S224DF-v3.6-build382, Flash Erase:[100], Flash Write:[100]
S224DF3X17000238                        Running : S224DF-v3.6.1-build372,170620 (GA)
Next Boot : S224DF-v3.6-build382, Flash Erase:[100], Flash Write:[100]
S124DP3X15000118                        Running : S124DP-v3.6.1-build372,170620 (GA)
Next Boot : S124DP-v3.6-build382, Flash Erase:[100], Flash Write:[100]
S124DP3X15000380                        Running : S124DP-v3.6.1-build372,170620 (GA)
Next Boot : S124DP-v3.6-build382, Flash Erase:[100], Flash Write:[100]
```

6. Restart the FortiSwitches after a 2-minute delay. For example:

```
execute switch-controller restart-swtp-delayed ALL
```

7. When the FortiSwitches are running again, check that they are running the new firmware version. For example:

```
execute switch-controller get-conn-status
Managed-devices in current vdom root:

STACK-NAME: FortiSwitch-Stack-flink
SWITCH-ID        VERSION    STATUS           ADDRESS         JOIN-TIME
NAME
S124DP3X15000118 v3.6.2     Authorized/Up    169.254.1.5     Mon Oct  2 15:26:51 2017     -
S124DP3X15000380 v3.6.2     Authorized/Up    169.254.1.4     Mon Oct  2 15:26:49 2017     -
S224DF3X16001718 v3.6.2     Authorized/Up    169.254.1.3     Mon Oct  2 15:25:44 2017     -
S224DF3X17000238 v3.6.2     Authorized/Up    169.254.1.2     Mon Oct  2 15:25:27 2017     -
```

Transitioning from a FortiLink split interface to a FortiLink MCLAG

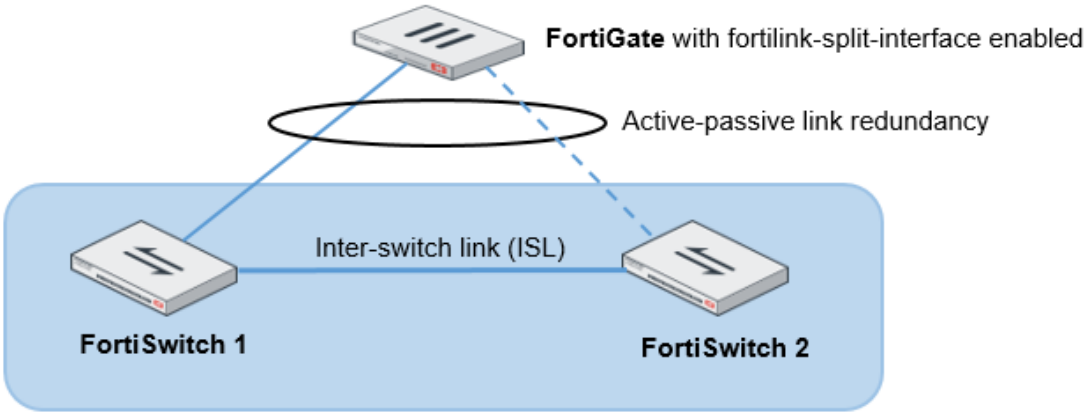
In this topology, the FortiLink split interface connects a FortiLink aggregate interface from one FortiGate to two FortiSwitches.

Note the following:

- This procedure also applies to a FortiGate in HA mode.
- More links can be added between the FortiGate and FortiSwitch.
- After the MCLAG is set up, only connect the tier-2 FortiSwitches.

1. Enable the split interface on the FortiLink aggregate interface. By default, the split interface is enabled. For example:

```
config system interface
   edit flinksplit1
      set ip 169.254.3.1 255.255.255.0
      set allowaccess ping capwap https
      set vlanforward enable
      set type aggregate
      set member port4 port5
      set lacp-mode static
      set fortilink enable
      set fortilink-split-interface enable
   next
end
```



2. Log into FortiSwitch 2 using the **Connect to CLI** button in the FortiGate GUI, use the `get switch lldp auto-isl-status` command to find out the name of the trunk connecting the peer switches, and change the ISL to an ICL. For example:

```
get switch lldp auto-isl-status

config switch trunk
   edit <trunk_name>
      set mclag-icl enable
   next
end
```

3. Log into FortiSwitch 1 using the **Connect to CLI** button in the FortiGate GUI, use the `get switch lldp auto-isl-status` command to find out the name of the trunk connecting the peer switches, and change the ISL to an ICL. For example:

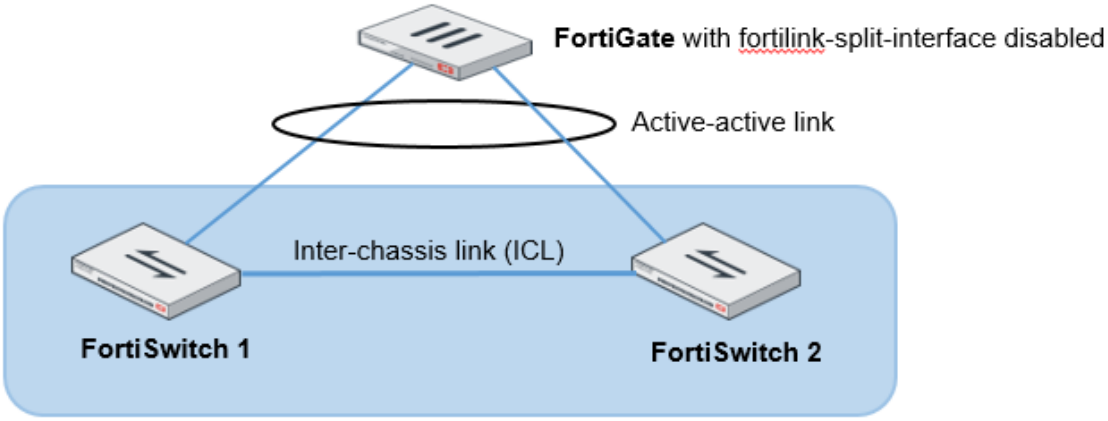
```
get switch lldp auto-isl-status

config switch trunk
   edit <trunk_name>
      set mclag-icl enable
   next
end
```

4. Log into the FortiGate and disable the split interface. For example:

```
config system interface
   edit flinksplit1
      set fortilink-split-interface disable
   next
end
```

5. Enable the LACP active mode.
6. Check that the LAG is working correctly. For example:

```
diagnose netlink aggregate name <aggregate_name>
```



Optional setup tasks

This section describes the following tasks:

- Configuring the FortiSwitch management port
- Converting to the FortiSwitch standalone mode
- Changing the admin password on the FortiGate for all managed FortiSwitches

Configuring the FortiSwitch management port

If the FortiSwitch model has a dedicated management port, you can configure remote management to the FortiSwitch. In FortiLink mode, the FortiGate is the default gateway, so you need to configure an explicit route for the FortiSwitch management port.

Using the Web administration GUI

1. Go to **Network > Static Routes** > **Create New > Route**.
2. Set **Destination** to **Subnet** and enter a subnetwork and mask.
3. Set **Device** to the management interface.
4. Add a **Gateway** IP address.

Using the FortiSwitch CLI

Enter the following commands:

```
config router static
   edit 1
      set device mgmt
      set gateway <router IP address>
      set dst <router subnet> <subnet mask>
   end
end
```

In the following example, the FortiSwitch management port is connected to a router with IP address 192.168.0.10:

```
config router static
   edit 1
      set device mgmt
      set gateway 192.168.0.10
      set dst 192.168.0.0 255.255.0.0
   end
end
```

Converting to FortiSwitch standalone mode

Use one of the following commands to convert a FortiSwitch from FortiLink mode to standalone mode so that it will no longer be managed by a FortiGate:

- `execute switch-controller factory-reset <switch-id>`
  This command returns the FortiSwitch to the factory defaults and then reboots the FortiSwitch. If the FortiSwitch is configured for FortiLink auto-discovery, FortiGate can detect and automatically authorize the FortiSwitch. For example:
  `execute switch-controller factory-reset S1234567890`
- `execute switch-controller set-standalone <switch-id>`
  This command returns the FortiSwitch to the factory defaults, reboots the FortiSwitch, and prevents the FortiGate from automatically detecting and authorizing the FortiSwitch. For example:
  `execute switch-controller set-standalone S1234567890`

You can disable FortiLink auto-discovery on multiple FortiSwitches using the following commands:

```
config switch-controller global
   set disable-discovery <switch-id>
end
```

For example:

```
config switch-controller global
   set disable-discovery S1234567890
end
```

You can also add or remove entries from the list of FortiSwitches that have FortiLink auto-discovery disabled using the following commands:

```
config switch-controller global
   append disable-discovery <switch-id>
   unselect disable-discovery <switch-id>
end
```

For example:

```
config switch-controller global
   append disable-discovery S012345678
   unselect disable-discovery S1234567890
end
```

Changing the admin password on the FortiGate for all managed FortiSwitches

By default, each FortiSwitch has an admin account without a password. To replace the admin passwords for all FortiSwitches managed by a FortiGate, use the following commands from the FortiGate CLI:

```
config switch-controller switch-profile
   edit default
      set login-passwd-override {enable | disable}
      set login-passwd <password>
```

```
    next
end
```

If you had already applied a profile with the override enabled and the password set and then decide to remove the admin password, you need to apply a profile with the override enabled and no password set; otherwise, your previously set password will remain in the FortiSwitch. For example:

```
config switch-controller switch-profile
   edit default
      set login-passwd-override enable
      unset login-passwd
   next
end
```

FortiSwitch features configuration

This section describes how to configure global FortiSwitch settings using FortiGate CLI commands. These settings will apply to all of the managed FortiSwitches. You can also override some of the settings on individual FortiSwitches.

VLAN configuration

Use Virtual Local Area Networks (VLANs) to logically separate a LAN into smaller broadcast domains. VLANs allow you to define different policies for different types of users and to set finer control on the LAN traffic. (Traffic is only sent automatically within the VLAN. You must configure routing for traffic between VLANs.)

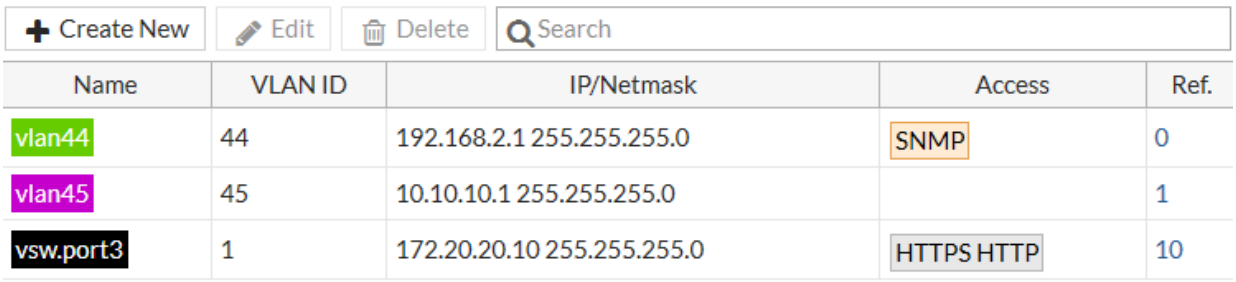
From the FortiGate, you can centrally configure and manage VLANs for the managed FortiSwitches.

In FortiSwitchOS 3.3.0 and later releases, the FortiSwitch supports untagged and tagged frames in FortiLink mode. The switch supports up to 1,023 user-defined VLANs. You can assign a VLAN number (ranging from 1-4095) to each of the VLANs.

You can configure the default VLAN for each FortiSwitch port as well as a set of allowed VLANs for each FortiSwitch port.

FortiSwitch VLANs display

The **WiFi & Switch Controller > FortiSwitch VLANs** page displays VLAN information for the managed switches.



Each entry in the VLAN list displays the following information:

- **Name** - name of the VLAN
- **VLAN ID** - the VLAN number
- **IP/Netmask** - address and mask of the subnetwork that corresponds to this VLAN
- **Access** - administrative access settings for the VLAN
- **Ref** - number of configuration objects referencing this VLAN

Enabling and disabling switch-controller access VLANs through FortiGate

Access VLANs are VLANs that aggregate client traffic solely to the FortiGate. This prevents direct client-to-client traffic visibility at the layer-2 VLAN layer. Clients can only communicate with the FortiGate. After the client traffic reaches the FortiGate, the FortiGate can then determine whether to allow various levels of access to the client by shifting the client's network VLAN as appropriate.

Use `enable` to allow traffic only to and from the FortiGate and to block FortiSwitch port-to-port traffic on the specified VLAN. Use `disable` to allow normal traffic on the specified VLAN.

```
config system interface
   edit <VLAN name>
      set switch-controller-access-vlan {enable | disable}
   next
end
```

Creating VLANs

Setting up a VLAN requires you to create the VLAN and assign FortiSwitch ports to the VLAN. You can do this with either the Web GUI or CLI.

Using the Web administration GUI

To create the VLAN:

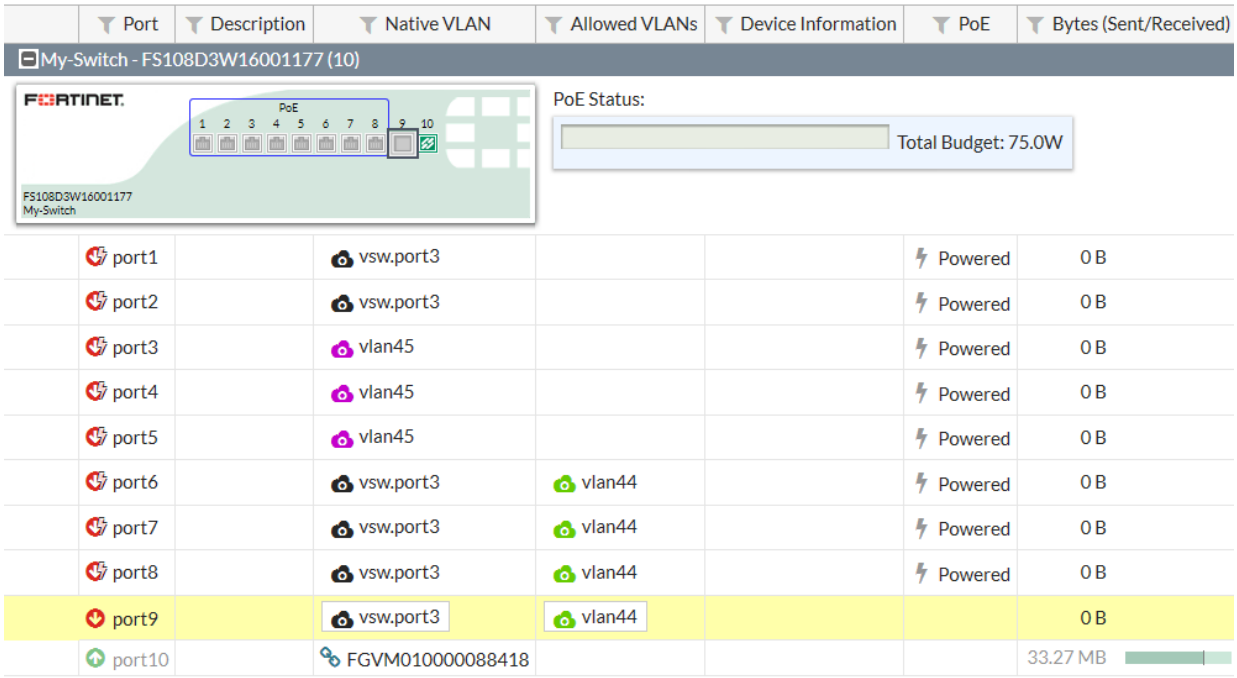
1. Go to **WiFi & Switch Controller > FortiSwitch VLANs**, select **Create New**, and change the following settings:

Interface Name	VLAN name
VLAN ID	Enter a number (1-4094)
Color	Choose a unique color for each VLAN, for ease of visual display.
IP/Network Mask	IP address and network mask for this VLAN.

2. Enable **DHCP Server** and set the IP range.
3. Set the **Admission Control** options as required.
4. Select **OK**.

To assign FortiSwitch ports to the VLAN:

1. Go to **WiFi & Switch Controller** > **FortiSwitch Ports**.
2. Click the desired port row.
3. Click the **Native VLAN** column in one of the selected entries to change the native VLAN.
4. Select a VLAN from the displayed list. The new value is assigned to the selected ports.
5. Click the **+** icon in the **Allowed VLANs** column to change the allowed VLANs.
6. Select one or more of the VLANs (or the value **all**) from the displayed list. The new value is assigned to the selected port.



Using the FortiSwitch CLI

1. Create the marketing VLAN.

```
config system interface
   edit <vlan name>
      set vlanid <1-4094>
      set color <1-32>
      set interface <FortiLink-enabled interface>
   end
```

2. Set the VLAN's IP address.

```
config system interface
   edit <vlan name>
      set ip <IP address> <Network mask>
   end
```

3. Enable a DHCP Server.

```
config system dhcp server
   edit 1
      set default-gateway <IP address>
      set dns-service default
      set interface <vlan name>
         config ip-range
            set start-ip <IP address>
            set end-ip <IP address>
         end
      set netmask <Network mask>
   end
```

4. Assign ports to the VLAN.

```
config switch-controller managed-switch
   edit <Switch ID>
```

```
            config ports
               edit <port name>
                  set vlan <vlan name>
                  set allowed-vlans <vlan name>
                  or
                  set allowed-vlans-all enable
               next
            end
         end
```

Assign untagged VLANs to a managed FortiSwitch port:

```
config switch-controller managed-switch
   edit <managed-switch>
      config ports
         edit <port>
            set untagged-vlans <VLAN-name>
         next
      end
   next
end
```

Configure MAC address aging interval

Use the following commands to configure how long an inactive MAC address is saved in the FortiSwitch hardware. The range is 10 to 1,000,000 seconds. The default value is 300. After this amount of time, the inactive MAC address is deleted from the FortiSwitch hardware.

```
config switch-controller global
   set mac-aging-interval <10 to 1000000>
end
```

Enable multiple FortiLink interfaces

NOTE: Only the first FortiLink interface has GUI support.

Use the following command to enable or disable multiple FortiLink interfaces.

```
config switch-controller global
   set allow-multiple-interfaces {enable | disable}
end
```

Configure IGMP settings

Use the following command to configure the global IGMP settings.

Aging time is the maximum number of seconds that the system will retain a multicast snooping entry. Enter an integer value from 15 to 3600. The default value is 300.

Flood-unknown-multicast controls whether the system will flood unknown multicast messages within the VLAN.

```
config switch-controller igmp-snooping
```

```
   set aging-time <15-3600>
   set flood-unknown-multicast {enable | disable}
end
```

Configure LLDP profiles

Use the following commands to configure LLDP profiles:

```
config switch-controller lldp-profile
   edit <profile number>
      set 802.1-tlvs port-vlan-id
      set 802.3-tlvs max-frame-size
      set auto-isl {enable | disable}
      set auto-isl-hello-timer <1-30>
      set auto-isl-port-group <0-9>
      set auto-isl-receive-timeout <3-90>
      set med-tlvs (inventory-management | network-policy)
end
```

Configure LLDP settings

Use the following commands to configure LLDP settings:

```
config switch-controller lldp-settings
   set status < enable | disable >
   set tx-hold <int>
   set tx-interval <int>
   set fast-start-interval <int>
   set management-interface {internal | management}
end
```

Variable	Description
status	Enable or disable
tx-hold	Number of tx-intervals before the local LLDP data expires. Therefore, the packet TTL (in seconds) is **tx-hold** times **tx-interval**. The range for tx-hold is 1 to 16, and the default value is 4.
tx-interval	How often the FortiSwitch transmits the LLDP PDU. The range is 5 to 4095 seconds, and the default is 30 seconds.
fast-start-interval	How often the FortiSwitch transmits the first 4 LLDP packets when a link comes up. The range is 2 to 5 seconds, and the default is 2 seconds. Set this variable to zero to disable fast start.
management-interface	Primary management interface to be advertised in LLDP and CDP PDUs.

Create LLDP asset tags for each managed FortiSwitch

You can use the following commands to add an LLDP asset tag for a managed FortiSwitch:

```
config switch-controller managed-switch
   edit <fsw>
      set switch-device-tag <string>
end
```

Add media endpoint discovery (MED) to an LLDP configuration

You can use the following commands to add media endpoint discovery (MED) features to an LLDP profile:

```
config switch-controller lldp-profile
   edit <lldp-profle>
        config med-network-policy
           edit guest-voice
              set status {disable | enable}
           next
           edit guest-voice-signaling
              set status {disable | enable}
           next
           edit guest-voice-signaling
              set status {disable | enable}
           next
           edit softphone-voice
              set status {disable | enable}
           next
           edit streaming-video
              set status {disable | enable}
           next
           edit video-conferencing
              set status {disable | enable}
           next
           edit video-signaling
              set status {disable | enable}
           next
           edit voice
              set status {disable | enable}
           next
           edit voice-signaling
              set status {disable | enable}
           end
        config custom-tlvs
           edit <name>
              set oui <identifier>
              set subtype <subtype>
              set information-string <string>
           end
      end
```

Display LLDP information

You can use the following commands to display LLDP information:

```
diagnose switch-controller dump lldp stats <switch> <port>
```

```
diagnose switch-controller dump lldp neighbors-summary <switch>
diagnose switch-controller dump lldp neighbors-detail <switch>
```

Configure the MAC sync interval

Use the following commands to configure the global MAC synch interval.

The MAC sync interval is the time interval between MAC synchronizations. The range is 30 to 600 seconds, and the default value is 60.

```
config switch-controller mac-sync-settings
   set mac-sync-interval <30-600>
end
```

Configure STP settings

Use the following CLI commands for global STP configuration. This configuration applies to all managed FortiSwitches:

```
config switch-controller stp-settings
   set name <name>
   set revision <stp revision>
   set hello-time <hello time>
   set forward-time <forwarding delay>
   set max-age <maximum aging time>
   set max-hops <maximum number of hops>
end
```

You can override the global STP settings for a FortiSwitch using the following commands:

```
config switch-controller managed-switch
   edit <switch-id>
      config stp-settings
         set local-override enable
```

Quarantines

Quarantined MAC addresses are blocked on the connected FortiSwitches from the network and the LAN.

Quarantining a MAC address

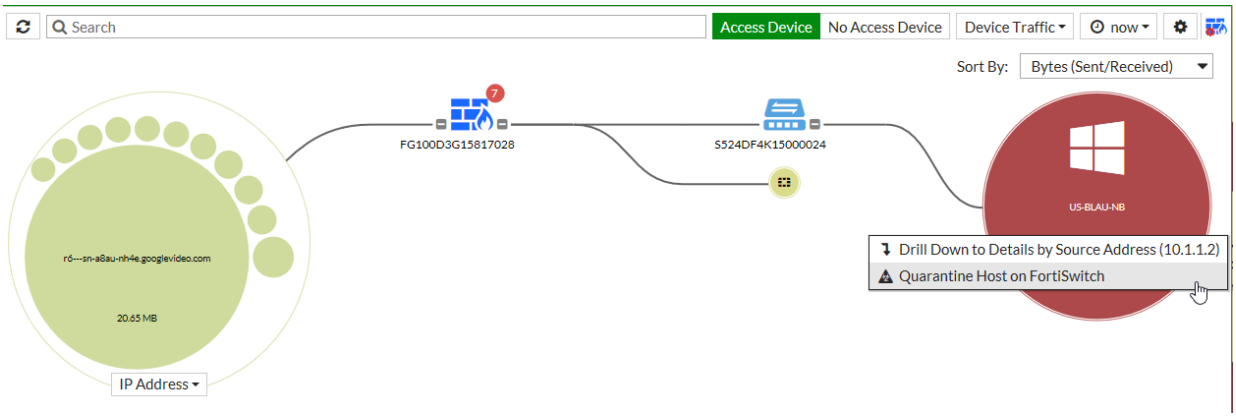
Using the FortiGate GUI

In the FortiGate GUI, the quarantine feature is automatically enabled when you quarantine a host.

1. Select the host to quarantine.
   - Go to **Security Fabric > Physical Topology**, right-click on a host, and select **Quarantine Host on FortiSwitch**.

- Go to **Security Fabric > Logical Topology**, right-click on a host, and select **Quarantine Host on FortiSwitch**.
- Go to **FortiView > Sources**, right-click on an entry in the Source column, and select **Quarantine Host on FortiSwitch**.

2. Click **OK** to confirm that you want to quarantine the host.



Using the FortiGate CLI

You must enable the quarantine feature in the FortiGate CLI using the `set quarantine enable` command. You can add MAC addresses to the quarantine list before enabling the quarantine feature, but the quarantine does not go into effect until enabled.

```
config switch-controller quarantine
   set quarantine enable
   config targets
      edit <MAC_address>
         set description <string>
         set tags <tag1 tag2 tag3 ...>
      next
   end
end
```

Option	Description
MAC_address	A layer-2 MAC address in the following format: `12:34:56:aa:bb:cc`
string	Optional. A description of the MAC address being quarantined.
tag1 tag2 tag3 ...	Optional. A list of arbitrary strings.

For example:

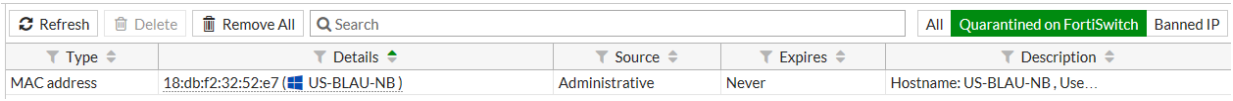
```
config switch-controller quarantine
   set quarantine enable
   config targets
      edit 00:00:00:aa:bb:cc
         set description "infected by virus"
         set tags "quarantined"
      next
   end
end
```

Viewing quarantine entries

Quarantine entries are created on the FortiGate that is managing the FortiSwitch.

Using the FortiGate GUI

1. Go to **Monitor > Quarantine Monitor**.
2. Click **Quarantined on FortiSwitch**.
   The Quarantined on FortiSwitch button is only available if a device is detected behind the FortiSwitch, which requires Device Detection to be enabled.



Using the FortiGate CLI

Use the following command to view the quarantine list of MAC addresses:

```
show switch-controller quarantine
```

For example:

```
show switch-controller quarantine

config switch-controller quarantine
   set quarantine enable
   config targets
      edit 00:11:22:33:44:55
      next
      edit 00:01:02:03:04:05
      next
   end
end
```

When the quarantine feature is enabled on the FortiGate, it creates a quarantine VLAN (qtn.<FortiLink_port_name>) on the virtual domain. The quarantine VLAN is applied to the allowed and untagged VLANs on all connected FortiSwitch ports.

Use the following command to view the quarantine VLAN:

```
show system interface qtn.<FortiLink_port_name>
```

For example:

```
show system interface qtn.port7

config system interface
   edit "qtn.port7"
      set vdom "vdom1"
      set description "Quarantine VLAN"
      set security-mode captive-portal
      set replacemsg-override-group "auth-intf-qtn.port7"
      set device-identification enable
      set device-identification-active-scan enable
      set snmp-index 34
```

```
        set switch-controller-access-vlan enable
        set color 6
        set interface "port7"
        set vlanid 4093
    next
end
```

Use the following command to view how the quarantine VLAN is applied to the allowed and untagged VLANs on all connected FortiSwitch ports:

```
show switch-controller managed-switch
```

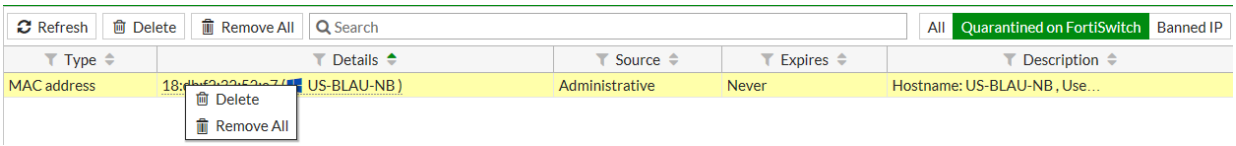
For example:

```
show switch-controller managed-switch

config switch-controller managed-switch
    edit "FS1D483Z15000036"
        set fsw-wan1-peer "port7"
        set fsw-wan1-admin enable
        set version 1
        set dynamic-capability 503
        config ports
            edit "port1"
                set vlan "vsw.port7"
                set allowed-vlans "qtn.port7"
                set untagged-vlans "qtn.port7"
            next
            edit "port2"
                set vlan "vsw.port7"
                set allowed-vlans "qtn.port7"
                set untagged-vlans "qtn.port7"
            next
            edit "port3"
                set vlan "vsw.port7"
                set allowed-vlans "qtn.port7"
                set untagged-vlans "qtn.port7"
            next
            ...
    end
end
```

Releasing MAC addresses from quarantine

Using the FortiGate GUI

1. Go to **Monitor > Quarantine Monitor**.
2. Click **Quarantined on FortiSwitch**.
3. Right-click on one of the entries and select **Delete** or **Remove All**.
4. Click **OK** to confirm your choice.



Using the FortiGate CLI

Use the following commands to delete a quarantined MAC address:

```
config switch-controller quarantine
config targets
   delete <MAC_address>
end
```

When the quarantine feature is disabled, all quarantined MAC addresses are released from quarantine. Use the following commands to disable the quarantine feature:

```
config switch-controller quarantine
   set quarantine disable
end
```

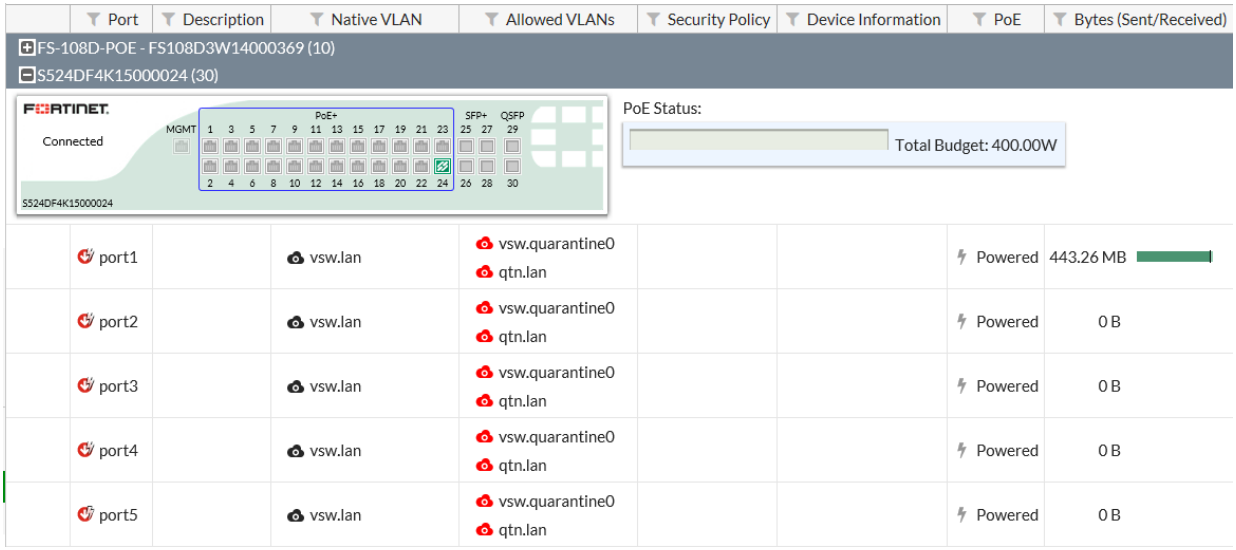
FortiSwitch port features

You can configure the FortiSwitch port feature settings from the FortiGate using the FortiSwitch CLI or Web administration GUI.

FortiSwitch ports display

The **WiFi & Switch Controller > FortiSwitch Ports** page displays port information about each of the managed switches.

The following figure shows the display for a FortiSwitch 524D-FPOE:

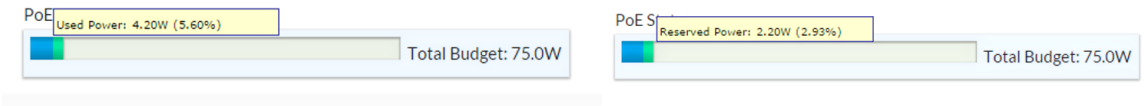


The switch faceplate displays:

- active ports (green)
- PoE-enabled ports (blue rectangle)
- FortiLink port (link icon)

PoE Status displays the total power budget and the actual power currently allocated.

The allocated power displays a blue bar for the used power (currently being consumed) and a green bar for the reserved power (power available for additional devices on the POE ports). See the following figures:



Each entry in the port list displays the following information:

- Port status (red for down, green for up)
- Port name
- Native VLAN
- Allowed VLANs
- Device information
- PoE status
- Bytes sent and received by the port

Configuring ports using the GUI

You can use the **WiFi & Switch Controller > FortiSwitch Ports** page to do the following with FortiSwitch switch ports:

- Set the native VLAN and add more VLANs
- Edit the description of the port
- Enable or disable the port
- Enable or disable PoE for the port
- Enable or disable DHCP blocking (if supported by the port)
- Enable or disable IGMP snooping (if supported by the port)
- Enable or disable whether a port is an edge port
- Enable or disable STP (if supported by the port)
- Enable or disable loop guard (if supported by the port)
- Enable or disable STP BPDU guard (if supported by the port)
- Enable or disable STP root guard (if supported by the port)

Resetting PoE-enabled ports

If you need to reset PoE-enabled ports, go to **WiFi & Switch Control > FortiSwitch Ports**, right-click on one or more PoE-enabled ports and select **Reset PoE** from the context menu.

You can also go to **WiFi & Switch Control > Managed FortiSwitch** and click on a port icon for the FortiSwitch of interest. In the FortiSwitch Ports page, right-click on one or more PoE-enabled ports and select **Reset PoE** from the context menu.

Configuring ports using the FortiGate CLI

You can configure the following FortiSwitch port settings using the FortiGate CLI:

- Configuring port speed and status on page 71
- Configure a VLAN on the port (see VLAN configuration)
- Configuring the DHCP trust setting on page 71
- Configuring PoE on page 72
- Configuring edge ports on page 72

Configuring port speed and status

Use the following commands to set port speed and other base port settings:

```
config switch-controller managed-switch
   edit <switch>
      config ports
         edit <port>
            set description <text>
            set speed <speed>
            set status {down | up}
         end
      end
```

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
      config ports
         edit port1
            set description "First port"
            set speed auto
            set status up
         end
      end
```

Configuring the DHCP trust setting

The DHCP blocking feature monitors the DHCP traffic from untrusted sources (for example, typically host ports and unknown DHCP servers) that might initiate traffic attacks or other hostile actions. To prevent this, DHCP blocking filters messages on untrusted ports.

Set the port as a trusted or untrusted DHCP-snooping interface:

```
config switch-controller managed-switch
   edit <switch-id>
      config ports
         edit <port name>
            set dhcp-snooping {trusted | untrusted}
         end
      end
```

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
      config ports
         edit port1
            set dhcp-snooping trusted
```

```
      end
   end
```

Configuring PoE

The following PoE CLI commands are available starting in FortiSwitchOS 3.3.0.

Enable PoE on the port

```
config switch-controller managed-switch
   edit <switch-id>
      config ports
         edit <port name>
            set poe-status {enable | disable}
         end
      end
```

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
      config ports
         edit port1
            set poe-status enable
         end
      end
```

Reset the PoE port

Power over Ethernet (PoE) describes any system that passes electric power along with data on twisted pair Ethernet cabling. Doing this allows a single cable to provide both data connection and electric power to devices (for example, wireless access points, IP cameras, and VoIP phones).

The following command resets PoE on the port:

```
execute switch-controller poe-reset <fortiswitch-id> <port>
```

Display general PoE status

```
get switch-controller <fortiswitch-id> <port>
```

The following example displays the PoE status for port 6 on the specified switch:

```
# get switch-controller poe FS108D3W14000967 port6
Port(6) Power:3.90W, Power-Status: Delivering Power
Power-Up Mode: Normal Mode
Remote Power Device Type: IEEE802.3AT PD
Power Class: 4
Defined Max Power: 30.0W, Priority:3
Voltage: 54.00V
Current: 78mA
```

Configuring edge ports

Use the following commands to enable or disable an interface as an edge port:

```
config switch-controller managed-switch
```

```
edit <switch>
   config ports
      edit <port>
         set edge-port {enable | disable}
         end
         end
```

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
      config ports
         edit port1
            set edge-port enable
         end
      end
```

Configuring STP

Starting with FortiSwitch Release 3.4.2, STP is enabled by default for the non-FortiLink ports on the managed FortiSwitches. STP is a link-management protocol that ensures a loop-free layer-2 network topology.

To configure global STP settings, see Configure STP settings on page 64.

Use the following commands to enable or disable STP on FortiSwitch ports:

```
config switch-controller managed-switch
   edit <switch-id>
      config ports
         edit <port name>
            set stp-state {enabled | disabled}
         end
      end
```

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
      config ports
         edit port1
            set stp-state enabled
         end
      end
```

To check the STP configuration on a FortiSwitch, use the following command:

```
diagnose switch-controller dump stp <FortiSwitch_serial_number> <instance_number>
```

For example:

```
FG100D3G15817028 # diagnose switch-controller dump stp S524DF4K15000024 0

MST Instance Information, primary-Channel:

Instance ID :   0

Switch Priority : 24576

Root MAC Address :    085b0ef195e4
Root Priority:    24576
```

```
Root Pathcost:    0
Regional Root MAC Address :   085b0ef195e4
Regional Root Priority:   24576
Regional Root Path Cost:  0
Remaining Hops:       20
This Bridge MAC Address :    085b0ef195e4
This bridge is the root

Port               Speed   Cost       Priority   Role         State       Edge  STP-Status  Loop
Protection
_________________  ______  _________  _________  ___________  __________  ____  __________  ________

port1              -       200000000  128        DISABLED     DISCARDING  YES     ENABLED         NO
port2              -       200000000  128        DISABLED     DISCARDING  YES     ENABLED         NO
port3              -       200000000  128        DISABLED     DISCARDING  YES     ENABLED         NO
port4              -       200000000  128        DISABLED     DISCARDING  YES     ENABLED         NO
port5              -       200000000  128        DISABLED     DISCARDING  YES     ENABLED         NO
port6              -       200000000  128        DISABLED     DISCARDING  YES     ENABLED         NO
port7              -       200000000  128        DISABLED     DISCARDING  YES     ENABLED         NO
port8              -       200000000  128        DISABLED     DISCARDING  YES     ENABLED         NO
port9              -       200000000  128        DISABLED     DISCARDING  YES     ENABLED         NO
port10             -       200000000  128        DISABLED     DISCARDING  YES     ENABLED         NO
port11             -       200000000  128        DISABLED     DISCARDING  YES     ENABLED         NO
port12             -       200000000  128        DISABLED     DISCARDING  YES     ENABLED         NO
port13             -       200000000  128        DISABLED     DISCARDING  YES     ENABLED         NO
port14             -       200000000  128        DISABLED     DISCARDING  YES     ENABLED         NO
port15             -       200000000  128        DISABLED     DISCARDING  YES     ENABLED         NO
port16             -       200000000  128        DISABLED     DISCARDING  YES     ENABLED         NO
port17             -       200000000  128        DISABLED     DISCARDING  YES     ENABLED         NO
port18             -       200000000  128        DISABLED     DISCARDING  YES     ENABLED         NO
port19             -       200000000  128        DISABLED     DISCARDING  YES     ENABLED         NO
port20             -       200000000  128        DISABLED     DISCARDING  YES     ENABLED         NO
port21             -       200000000  128        DISABLED     DISCARDING  YES     ENABLED         NO
port22             -       200000000  128        DISABLED     DISCARDING  YES     ENABLED         NO
port23             -       200000000  128        DISABLED     DISCARDING  YES     ENABLED         NO
port25             -       200000000  128        DISABLED     DISCARDING  YES     ENABLED         NO
port26             -       200000000  128        DISABLED     DISCARDING  YES     ENABLED         NO
port27             -       200000000  128        DISABLED     DISCARDING  YES     ENABLED         NO
port28             -       200000000  128        DISABLED     DISCARDING  YES     ENABLED         NO
port29             -       200000000  128        DISABLED     DISCARDING  YES     ENABLED         NO
port30             -       200000000  128        DISABLED     DISCARDING  YES     ENABLED         NO
internal           1G      20000      128        DESIGNATED   FORWARDING  YES     DISABLED        NO
__FoRtI1LiNk0__    1G      20000      128        DESIGNATED   FORWARDING  YES     DISABLED        NO
```

Configuring STP root guard

Root guard protects the interface on which it is enabled from becoming the path to root. When enabled on an interface, superior BPDUs received on that interface are ignored or dropped. Without using root guard, any switch that participates in STP maintains the ability to reroute the path to root. Rerouting might cause your network to transmit large amounts of traffic across suboptimal links or allow a malicious or misconfigured device to pose a security risk by passing core traffic through an insecure device for packet capture or inspection. By enabling root guard on multiple interfaces, you can create a perimeter around your existing paths to root to enforce the specified network topology.

Enable root guard on all ports that should not be root bridges. Do not enable root guard on the root port. You must have STP enabled to be able to use root guard.

Use the following commands to enable or disable STP root guard on FortiSwitch ports:

```
config switch-controller managed-switch
   edit <switch-id>
      config ports
         edit <port name>
            set stp-root-guard {enabled | disabled}
         end
```

```
        end
```

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
      config ports
         edit port1
            set stp-root-guard enabled
         end
      end
```

Configuring STP BPDU guard

Similar to root guard, BPDU guard protects the designed network topology. When BPDU guard is enabled on STP edge ports, any BPDUs received cause the ports to go down for a specified number of minutes. The BPDUs are not forwarded, and the network edge is enforced.

There are two prerequisites for using BPDU guard:

- You must define the port as an edge port with the `set edge-port enable` command.
- You must enable STP on the switch interface with the `set stp-state enabled` command.

You can set how long the port will go down when a BPDU is received for a maximum of 120 minutes. The default port timeout is 5 minutes. If you set the timeout value to 0, the port will not go down when a BPDU is received, but you will have manually reset the port.

Use the following commands to enable or disable STP BPDU guard on FortiSwitch ports:

```
config switch-controller managed-switch
   edit <switch-id>
      config ports
         edit <port name>
            set stp-bpdu-guard {enabled | disabled}
            set stp-bpdu-guard-time <0-120>
         end
      end
```

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
      config ports
         edit port1
            set stp-bpdu-guard enabled
            set stp-bpdu-guard-time 10
         end
      end
```

To check the configuration of STP BPDU guard on a FortiSwitch, use the following command:

```
diagnose switch-controller dump bpdu-guard-status <FortiSwitch_serial_number>
```

For example:

```
FG100D3G15817028 # diagnose switch-controller dump bpdu-guard-status
S524DF4K15000024
```

```
Managed Switch : S524DF4K15000024 0

Portname              State      Status       Timeout(m)     Count    Last-Event
__________________    _______    _________    ___________    _____    ______________

port1                 enabled      -              10           0          -
port2                 disabled     -              -            -          -
port3                 disabled     -              -            -          -
port4                 disabled     -              -            -          -
port5                 disabled     -              -            -          -
port6                 disabled     -              -            -          -
port7                 disabled     -              -            -          -
port8                 disabled     -              -            -          -
port9                 disabled     -              -            -          -
port10                disabled     -              -            -          -
port11                disabled     -              -            -          -
port12                disabled     -              -            -          -
port13                disabled     -              -            -          -
port14                disabled     -              -            -          -
port15                disabled     -              -            -          -
port16                disabled     -              -            -          -
port17                disabled     -              -            -          -
port18                disabled     -              -            -          -
port19                disabled     -              -            -          -
port20                disabled     -              -            -          -
port21                disabled     -              -            -          -
port22                disabled     -              -            -          -
port23                disabled     -              -            -          -
port25                disabled     -              -            -          -
port26                disabled     -              -            -          -
port27                disabled     -              -            -          -
port28                disabled     -              -            -          -
port29                disabled     -              -            -          -
port30                disabled     -              -            -          -
__FoRtI1LiNk0__       disabled     -              -            -          -
```

Configuring loop guard

A loop in a layer-2 network results in broadcast storms that have far-reaching and unwanted effects. Fortinet loop guard helps to prevent loops. When loop guard is enabled on a switch port, the port monitors its subtending network for any downstream loops. The loop guard feature is designed to work in concert with STP rather than as a replacement for STP. By default, loop guard is disabled on all ports.

Use the following commands to configure loop guard on a FortiSwitch port:

```
config switch-controller managed-switch
   edit <switch-id>
      config ports
         edit <port name>
            set loop-guard {enabled | disabled}
         end
      end
```

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
      config ports
         edit port1
            set stp-bpdu-guard enabled
            set stp-bpdu-guard-time 10
         end
      end
```

Configuring LLDP settings

The Fortinet data center switches support the Link Layer Discovery Protocol (LLDP) for transmission and reception wherein the switch will multicast LLDP packets to advertise its identity and capabilities. A switch receives the equivalent information from adjacent layer-2 peers.

Use the following commands to configure LLDP on a FortiSwitch port:

```
config switch-controller managed-switch
   edit <switch-id>
      config ports
         edit <port name>
            set lldp-status {rx-only | tx-only | tx-rx | disable}
            set lldp-profile <profile name>
         end
      end
```

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
      config ports
         edit port2
            set lldp-status tx-rx
            set lldp-profile default
         end
      end
```

Configuring IGMP settings

IGMP snooping allows the FortiSwitch to passively listen to the Internet Group Management Protocol (IGMP) network traffic between hosts and routers. The switch uses this information to determine which ports are interested in receiving each multicast feed. FortiSwitch can reduce unnecessary multicast traffic on the LAN by pruning multicast traffic from links that do not contain a multicast listener.

```
config switch-controller managed-switch
   edit <switch-id>
      config ports
         edit <port name>
            set igmp-snooping {enable | disable}
            set igmps-flood-reports {enable | disable}
         end
      end
```

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
      config ports
         edit port3
            set igmp-snooping enable
            set igmps-flood-reports enable
         end
      end
```

FortiSwitch port security policy

The features listed here are valuable in endpoint authorization and access-control within a retail/enterprise LAN environment. In a FortiLink setup, you can configure these capabilities from the FortiGate while endpoints are connected to switch ports.

NOTE: In FortiLink mode, you must manually create a firewall policy to allow RADIUS traffic for 802.1x authentication from the FortiSwitch (for example, from the FortiLink interface) to the RADIUS server through the FortiGate.

End devices fall into two supported categories: one that supports 8021.X client and one that does not.

Before the Managed Release 5.6.0, only the following configuration was supported per VLAN:

- 802.1X

With Managed Release 5.6.0, additional port security features are available:

- Move 802.1X control from VLAN to port
  - Previously, only one VLAN could be assigned to one port. With both tagged and untagged VLANs allowed in 5.4.x, this is no longer suitable and will be migrated to the switch port.
  - Automatic configuration migration is supported.
- Support for client-less devices using mac-auth-bypass (MAB)
  - For devices that are incapable of supporting EAPoL/EAP, FortiSwitch will conduct the authentication on behalf of the device. A maximum of three concurrent MAB devices per port can exist.
- Multiple secured endpoints on single port
  - Enforcement is per MAC address
- Dynamic VLAN assignment
  - RADIUS-assigned VLANs
- Guest VLAN configuration
  - With authentication timeout
- RADIUS configuration
  - Set secret keys for primary and secondary servers.
- User configuration
  - Use a RADIUS server to authenticate users.
- Additional timers and modes
  - Re-authentication period
  - Maximum re-authentication attempts
  - Link down to un-authenticate

NOTE: In the following commands, "*" indicates the default setting.

Configure the 802.1X settings for a virtual domain

To configure the 802.1X security policy for a virtual domain, use the following commands:

```
config switch-controller 802-1X-settings
   set reauth-period < int >
   set max-reauth-attempt < int >
```

```
    set link-down-auth < *set-unauth | no-action >
end
```

Option	Description
`set link-down-auth`	If a link is down, this command determines the authentication state. Choosing `set-auth` sets the interface to unauthenticated when a link is down, and reauthentication is needed. Choosing `no-auth` means that the interface does not need to be reauthenticated when a link is down.
`set reauth-period`	This command sets how often reauthentication is needed. The range is 1-1440 minutes. The default is 60 minutes. Setting the value to 0 minutes disables reauthenticaion.
`set max-reauth-attempt`	This command sets the maximum number of reauthentication attempts. The range is 1-15. the default is 3. Setting the value to 0 disables reauthentication.

Override the virtual domain settings

You can override the virtual domain settings for the 802.1X security policy.

Using the FortiGate GUI

To override the 802.1X settings for a virtual domain:

1. Go to **WiFi & Switch Controller > Managed FortiSwitch**.
2. Click on a FortiSwitch faceplate and click **Edit**.
3. In the Edit Managed FortiSwitch page, move the **Override 802-1X settings** slider to the right.
4. In the Reauthentication Interval field, enter the number of minutes before reauthentication is required. The maximum interval is 1,440 minutes. Setting the value to 0 minutes disables reauthentiction.
5. In the Max Reauthentication Attempts field, enter the maximum times that reauthentication is attempted. The maximum number of attempts is 15. Setting the value to 0 disables reauthentication.
6. Select **Deauthenticate** or **None** for the link down action. Selecting **Deauthenticate** sets the interface to unauthenticated when a link is down, and reauthentication is needed. Selecting **None** means that the interface does not need to be reauthenticated when a link is down.
7. Click **OK**.

Using the FortiGate CLI

To override the 802.1X settings for a virtual domain, use the following commands:

```
config switch-controller managed-switch
   edit < switch >
      config 802-1X-settings
         set local-override [ enable | *disable ]
            set reauth-period < int >                  // visible if override enabled
            set max-reauth-attempt < int >             // visible if override enabled
            set link-down-auth < *set-unauth | no-action >   // visible if override enabled
      end
```

```
    next
end
```

For a description of the options, see Configure the 802.1X settings for a virtual domain.

Define an 802.1X security policy

You can define multiple 802.1X security policies.

Using the FortiGate GUI

To create an 802.1X security policy:

1. Go to **WiFi & Switch Controller > FortiSwitch Security Policies**.
2. Click **Create New**.
3. Enter a name for the new FortiSwitch security policy.
4. For the security mode, select **Port-based** or **MAC-based**.
5. Click **+** to select which user groups will have access.
6. Enable or disable guest VLANs on this interface to allow restricted access for some users.
7. Enter the number of seconds for authentication delay for guest VLANs. The range is 60-900 seconds.
8. Enable or disable authentication fail VLAN on this interface to allow restricted access for users who fail to access the guest VLAN.
9. Enable or disable MAC authentication bypass (MAB) on this interface.
10. Enable or disable EAP pass-through mode on this interface.
11. Enable or disable whether the session timeout for the RADIUS server will overwrite the local timeout.
12. Click **OK**.

Using the FortiGate CLI

To create an 802.1X security policy, use the following commands:

```
config switch-controller security-policy 802-1X
   edit "<policy.name>"
      set security-mode {802.1X | 802.1X-mac-based)
      set user-group <*group_name | Guest-group | SSO_Guest_Users>
      set mac-auth-bypass [enable | *disable]
      set eap-passthru [enable | disable]
      set guest-vlan [enable | *disable]
      set guest-vlan-id "guest-VLAN-name"
      set guest-auth-delay <integer>
      set auth-fail-vlan  [enable | *disable]
      set auth-fail-vlan-id "auth-fail-VLAN-name"
      set radius-timeout-overwrite [enable | *disable]
      set policy-type 802.1X
   end
end
```

Option	Description
`set security-mode`	You can restrict access with 802.1X port-based authentication or with 802.1X MAC-based authentication.
`set user-group`	You can set a specific group name, Guest-group, or SSO_Guest_Users to have access.
`set mac-auth-bypass`	You can enable or disable MAB on this interface.
`set eap-passthrough`	You can enable or disable EAP pass-through mode on this interface.
`set guest-vlan`	You can enable or disable guest VLANs on this interface to allow restricted access for some users.
`set guest-vlan-id "guest-VLAN-name"`	You can specify the name of the guest VLAN.
`set guest-auth-delay`	You can set the authentication delay for guest VLANs on this interface. The range is 60-900 seconds.
`set auth-fail-vlan`	You can enable or disable authentication fail VLAN on this interface to allow restricted access for users who fail to access the guest VLAN.
`set auth-fail-vlan-id "auth-fail-VLAN-name"`	You can specify the name of the authentication fail VLAN
`set radius-timeout-overwrite`	You can enable or disable whether the session timeout for the RADIUS server will overwrite the local timeout.
`set policy-type 802.1X`	You can set the policy type to the 802.1X security policy.

Apply an 802.1X security policy to a FortiSwitch port

You can apply a different 802.1X security policy to each FortiSwitch port.

Using the FortiGate GUI

To apply an 802.1X security policy to a managed FortiSwitch port:

1. Go to **WiFi & Switch Controller > FortiSwitch Ports**.
2. Click the **+** next to a FortiSwitch.
3. In the Security Policy column for a port, click + to select a security policy.
4. Click **OK** to apply the security policy to that port.

Using the FortiGate CLI

To apply an 802.1X security policy to a managed FortiSwitch port, use the following commands:

```
config switch-controller managed-switch
```

```
    edit <managed-switch>
      config ports
        edit <port>
          set port-security-policy <802.1X-policy>
        next
      end
    next
end
```

Additional capabilities

This chapter covers the following topics:

Execute custom FortiSwitch commands

From the FortiGate, you can execute FortiSwitch commands on the managed FortiSwitch.

This feature adds a simple scripting mechanism for users to execute generic commands on the switch.

NOTE: FortiOS 5.6.0 introduces additional capabilities related to the managed FortiSwitch.

Create a command

Use the following syntax to create a command file:

```
config switch-controller custom-command
   edit <cmd-name>
      set command " <FortiSwitch commands>"
```

Next, create a command file to set the STP max-age parameter:

```
config switch-controller custom-command
   edit "stp-age-10"
      set command "config switch stp setting
         set max-age 10
         end
      "
   next
end
```

Execute a command

After you have created a command file, use the following command on the FortiGate to execute the command file on the target switch:

```
exec switch-controller custom-command <cmd-name> <target-switch>
```

The following example runs the **stp-age-10** command on the specified target FortiSwitch:

```
# exec switch-controller custom-command stp-age-10 S124DP3X15000118
```

Firmware upgrade management and compatible version information

You can view the current firmware version of a FortiSwitch and upgrade the FortiSwitch to a new firmware version. FortiGate will suggest an upgrade when a new version is available in FortiGuard.

Using the FortiGate Web interface

To view the FortiSwitch firmware version:

1. Go to **WiFi & Switch Controller**>**Managed FortiSwitch**.
2. In the main panel, select the FortiSwitch and click **Edit**.
3. In the **Edit Managed FortiSwitch** panel, the **Firmware** section displays the current build on the FortiSwitch.

To update the FortiSwitch firmware version:

1. Click **Update** to open the **Update Firmware panel**.
2. Click **Select File**. In the file chooser, click the image file and click **Open**.
3. Click **Upload and Reboot** to install the new image and reboot the FortiSwitch.

Using the CLI

Use the following command to display the latest version:

```
diagnose fdsm fortisw-latest-ver <model>
```

Use the following command to download the image:

```
diagnose fdsm fortisw-download <image id>
```

The following example shows how to download the latest image for FS224D:

```
FG100D3G15801204 (global) # diagnose fdsm fortisw-latest-ver FS224D
FS224D - 3.4.2 b192 03004000FIMG0900904002FG100D3G15801204 (global) #

diagnose fdsm fortisw-download 03004000FIMG0900904002

Download image-03004000FIMG0900904002:
################################################################################
Result=Success
```

FortiSwitch log export

You can enable and disable the managed FortiSwitches to export their syslogs to the FortiGate. The setting is global, and the default setting is enabled. Starting in FortiOS 5.6.3, more details are included in the exported FortiSwitch logs.

To allow a level of filtering, FortiGate sets the user field to "fortiswitch-syslog" for each entry.

The following is the CLI command syntax:

```
config switch-controller switch-log
   set status (*enable | disable)
   set severity [emergency | alert | critical | error | warning | notification |
       *information | debug]
end
```

You can override the global log settings for a FortiSwitch, using the following commands:

```
config switch-controller managed-switch
   edit <switch-id>
      config switch-log
         set local-override enable
```

At this point, you can configure the log settings that apply to this specific switch.

FortiSwitch per-port device visibility

In the FortiGate GUI, **User & Device** > **Device List** displays a list of devices attached to the FortiSwitch ports. For each device, the table displays the IP address of the device and the interface (FortiSwitch name and port).

From the CLI, the following command displays information about the host devices:

```
diagnose switch-controller dump mac-hosts_switch-ports
```

FortiGate CLI support for FortiSwitch features (on non-FortiLink ports)

You can configure the following FortiSwitch features from the FortiGate CLI.

Configuring a link aggregation group (LAG)

You can configure a link aggregation group (LAG) for non-FortiLink ports on a FortiSwitch. You cannot configure ports from different FortiSwitches in one LAG.

```
config switch-controller managed-switch
   edit <switch-id>
      config ports
         it <trunk name>
            set type trunk
            set mode < static | lacp > Link Aggregation mode
            set bundle (enable | disable)
            set min-bundle <int>
            set max-bundle <int>
            set members < port1 port2 ...>
         next
      end
   end
end
```

Configuring an MCLAG with managed FortiSwitches

A multichassis LAG (MCLAG) provides node-level redundancy by grouping two FortiSwitch models together so that they appear as a single switch on the network. If either switch fails, the MCLAG continues to function without any interruption, increasing network resiliency and eliminating the delays associated with the Spanning Tree Protocol (STP). For the network topology, see Dual-homed servers connected to FortiLink tier-1 FortiSwitches using an MCLAG and Standalone FortiGate with dual-homed FortiSwitch access .

Notes

- Both peer switches should be of the same hardware model and same software version. Mismatched configurations might work but are unsupported.
- There is a maximum of two FortiSwitch models per MCLAG.
- The routing feature is not available within an MCLAG.
- For static MAC addresses within an MCLAG, if one FortiSwitch learns the MAC address, the second FortiSwitch will automatically learn the MAC address.

To configure an MCLAG with managed FortiSwitches:

1. For each MCLAG peer switch, log into the FortiSwitch to create a LAG:

```
config switch trunk
   edit "LAG-member"
      set mode lacp-active
      set mclag-icl enable
      set members "<port>" "<port>"
   next
```

2. Enable the MCLAG on each managed FortiSwitch:

```
config switch-controller managed-switch
   edit "<switch-id>"
      config ports
         edit "<trunk name>"
            set type trunk
            set mode {static | lacp-passive | lacp-active}
            set bundle {enable | disable}
            set members "<port>,<port>"
            set mclag {enable | disable}
         next
      end
   next
```

3. Log into each managed FortiSwitch to check the MCLAG configuration:

```
diagnose switch mclag
```

After the FortiSwitches are configured as MCLAG peer switches, any port that supports advanced features on the FortiSwitch can become a LAG port. When `mclag` is enabled and the LAG port names match, an MCLAG peer set is automatically formed. The member ports for each FortiSwitch in the MCLAG do not need to be identical to the member ports on the peer FortiSwitch.

Configuring storm control

Storm control uses the data rate (packets/sec, default 500) of the link to measure traffic activity, preventing traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a port.

When the data rate exceeds the configured threshold, storm control drops excess traffic. You can configure the types of traffic to drop: broadcast, unknown unicast, or multicast.

The storm control settings are global to all of the non-FortiLink ports on the managed switches. Use the following CLI commands to configure storm control:

```
config switch-controller storm-control
   set rate <rate>
   set unknown-unicast (enable | disable)
   set unknown-multicast (enable | disable)
   set broadcast (enable | disable)
end
```

You can override the global storm control settings for a FortiSwitch using the following commands:

```
config switch-controller managed-switch
   edit <switch-id>
      config storm-control
         set local-override enable
```

At this point, you can configure the storm control settings that apply to this specific switch.

Displaying port statistics

Port statistics will be accessed using the following FortiSwitch CLI command:

```
FG100D3G15804763 # diagnose switch-controller dump port-stats
S124DP3X16000413 port8
S124DP3X16000413 0 :
{
   "port8":{
      "tx-bytes":823526672,
      "tx-packets":1402390,
      "tx-ucast":49047,
      "tx-mcast":804545,
      "tx-bcast":548798,
      "tx-errors":0,
      "tx-drops":3,
      "tx-oversize":0,
      "rx-bytes":13941793,
      "rx-packets":160303,
      "rx-ucast":148652,
      "rx-mcast":7509,
      "rx-bcast":4142,
      "rx-errors":0,
      "rx-drops":720,
      "rx-oversize":0,
      "undersize":0,
      "fragments":0,
      "jabbers":0,
      "collisions":0,
```

```
        "crc-alignments":0,
        "l3packets":0
    }
}
```

Configuring QoS with managed FortiSwitches

Quality of Service (QoS) provides the ability to set particular priorities for different applications, users, or data flows.

NOTE: FortiGate does not support QoS for hard or soft switch ports.

FortiSwitch supports the following QoS configuration capabilities:

- Mapping the IEEE 802.1p and Layer 3 QoS values (Differentiated Services and IP Precedence) to an outbound QoS queue number.
- Providing eight egress queues on each port.
- Policing the maximum data rate of egress traffic on the interface.

To configure the QoS for managed FortiSwitches:

1. Configure a Dot1p map.

   A Dot1p map defines a mapping between IEEE 802.1p class of service (CoS) values (from incoming packets on a trusted interface) and the egress queue values. Values that are not explicitly included in the map will follow the default mapping, which maps each priority (0-7) to queue 0. If an incoming packet contains no CoS value, the switch assigns a CoS value of zero.

   NOTE: Do not enable trust for both Dot1p and DSCP at the same time on the same interface. If you do want to trust both Dot1p and IP-DSCP, the FortiSwitch uses the latter value (DSCP) to determine the queue. The switch will use the Dot1p value and mapping only if the packet contains no DSCP value.

   ```
   config switch-controller qos dot1p-map
      edit <Dot1p map name>
         set description <text>
         set priority-0 <queue number>
         set priority-1 <queue number>
         set priority-2 <queue number>
         set priority-3 <queue number>
         set priority-4 <queue number>
         set priority-5 <queue number>
         set priority-6 <queue number>
         set priority-7 <queue number>
      next
   end
   ```

2. Configure a DSCP map.

   A DSCP map defines a mapping between IP precedence or DSCP values and the egress queue values. For IP precedence, you have the following choices:
   - network-control—Network control
   - internetwork-control—Internetwork control
   - critic-ecp—Critic and emergency call processing (ECP)
   - flashoverride—Flash override

- flash—Flash
- immediate—Immediate
- priority—Priority
- routine—Routine

```
config switch-controller qos ip-dscp-map
   edit <DSCP map name>
      set description <text>
      configure map <map_name>
         edit <entry name>
            set cos-queue <COS queue number>
            set diffserv {CS0 | CS1 | AF11 | AF12 | AF13 | CS2 | AF21 | AF22 | AF23
                | CS3 | AF31 | AF32 | AF33 | CS4 | AF41 | AF42 | AF43 | CS5 | EF |
                CS6 | CS7}
            set ip-precedence {network-control | internetwork-control | critic-ecp
                | flashoverride | flash | immediate | priority | routine}
            set value <DSCP raw value>
         next
      end
   end
```

3. Configure the egress QoS policy.

In a QoS policy, you set the scheduling mode for the policy and configure one or more CoS queues. Each egress port supports eight queues, and three scheduling modes are available:

- With strict scheduling, the queues are served in descending order (of queue number), so higher number queues receive higher priority.
- In simple round-robin mode, the scheduler visits each backlogged queue, servicing a single packet from each queue before moving on to the next one.
- In weighted round-robin mode, each of the eight egress queues is assigned a weight value ranging from 0 to 63.

```
config switch-controller qos queue-policy
   edit <QoS egress policy name>
      set schedule {strict | round-robin | weighted}
      config cos-queue
      edit [queue-<number>]
         set description <text>
         set min-rate <rate in kbps>
         set max-rate <rate in kbps>
         set drop-policy {taildrop | random-early-detection}
         set weight <weight value>
         next
      end
   next
end
```

4. Configure the overall policy that will be applied to the switch ports.

```
config switch-controller qos qos-policy
   edit <QoS egress policy name>
      set default-cos <default CoS value 0-7>
      set trust-dot1p-map <Dot1p map name>
      set trust-ip-dscp-map <DSCP map name>
```

```
      set queue-policy <queue policy name>
   next
end
```

5. Configure each switch port.

```
config switch-controller managed-switch
   edit <switch-id>
      config ports
         edit <port>
            set qos-policy <CoS policy>
         next
      end
   next
end
```

Troubleshooting

Troubleshooting FortiLink issues

If the FortiGate does not establish the FortiLink connection with the FortiSwitch, perform the following troubleshooting checks.

Check the FortiGate configuration

To use the FortiGate GUI to check the FortiLink interface configuration:

1. In **Network** > **Interfaces**, double-click the interface used for FortiLink.
2. Ensure that **Dedicated to FortiSwitch** is set for this interface.

To use the FortiGate CLI to verify that you have configured the DHCP and NTP settings correctly:

1. Verify that the NTP server is enabled and that the FortiLink interface has been added to the list:

```
show system ntp
```

2. Ensure that the DHCP server on the Fortilink interface is configured correctly:

```
show system dhcp
```

Check the FortiSwitch configuration

To use FortiSwitch CLI commands to check the FortiSwitch configuration:

1. Verify that the switch system time matches the time on the FortiGate:

```
get system status
```

2. Verify that FortiGate has sent an IP address to the FortiSwitch (anticipate an IP address in the range 169.254.x.x):

```
get system interfaces
```

3. Verify that you can ping the FortiGate IP address:

```
exec ping x.x.x.x
```

To use FortiGate CLI commands to check the FortiSwitch configuration:

1. Verify that the connections from the FortiGate to the FortiSwitches are up:

```
exec switch-controller get-conn-status
```

2. Verify that ports for a specific FortiSwitch stack are connected to the correct locations:

```
exec switch-controller get-physical-conn <FortiSwitch-Stack-ID>
```

3. Verify that all the ports for a specific FortiSwitch are up:

```
exec switch-controller get-conn-status <FortiSwitch-device-ID>
```

FORTINET

High Performance Network Security